GOSDEN HOUSE SCHOOL ACCESSIBILITY PLAN

Gosden House School recognises and values the contributions that parents, carers, governors and other members of the community can make. We will endeavour to encourage the wider community to understand the aims and vision of the school and to involve them wherever possible.

Provision of information in other formats *- We will endeavour, wherever possible, to provide information in alternative formats when required or requested. Examples of this are by using email, royal mail, enlarged print versions, audio tapes, translations, symbolled text. Adequate prior notice would be required through the school office.*
Accessibility to premises *- To continue to ensure that the school building and grounds are accessible to the extended school community, pupils, staff, governors, parents and community members as far as reasonably possible.*

Online and Digital Safety Policy

Date and author of original policy	E Mainwaring Sep 2017
Review Date	Sep 2022
Next review date	Sep 2023 Annual review cycle
Current Authors	E Mainwaring C Almond
Date approved and signed in governing body meeting – (if applicable)	
Signed Chair of Governors- (if applicable)	Signed Head teacher Cindy O Sullivan

Contents

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Head teacher
- Online Safety Coordinator
- Technical support
- School Business Manager

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils – annual PSHE survey
    - parents / carers – organised by CA – snapshot survey on an annual basis so this is monitored and can drive any changes in policy
    - staff – survey and base support on this

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 of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. School will seek advice from the police in regards to this as and when it is needed (see appendix for template policy).In the case of both acts, school will work in partnership with parents/carers to educate, support and respond to individual incidents on a case-by-case basis.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/ carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the governing body will be nominated to join the online safety team. The responsibilities of their role will include -

- meetings with the Online Safety Co-ordinator
- meet with the online safety team
- aware that online safety incidents are being logged and monitored by safeguarding team
- reporting to relevant Governors meeting

Head teacher and Senior Leaders

- The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator/ DSLs.
- In the event of a serious allegation being made against a member of staff the head teacher will be alerted as referenced in our school safeguarding policy and the relevant procedure will be followed.
- The Head teacher and Senior Leaders are responsible for ensuring that the Online Safety Co-ordinator 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 and Senior Leaders 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. Supervision is available from the HSLW and Quandary Therapies.
- The Head teacher and Senior Leaders liaise with the Local Authority where necessary.

Online Safety Co-ordinator

- Leads the Online Safety Group
- has an awareness of online safety issues as logged by staff on cpoms
- Has a leading role in establishing and reviewing the school online safety policies and documents
- Provides training and advice for staff
- Provides training and advice for families

- Liaises with school technical staff i.e. Sweet haven and discuss technical support and updates i.e. filters
- Works closely with DSLs and Senior Leadership Team i.e. to ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident

Network Manager / Technical staff

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection in which passwords are regularly changed
- The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person that 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 network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher/ Deputy Head/ Online Safety Co-ordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Agreement (AUP)
- They report any suspected misuse or problem to the Head teacher; DSL or Online Safety Co-ordinator for investigation / action / sanction
- All digital communications with pupils and parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use agreements

- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (as agreed) and implement current policies with regard to these devices
- In lessons where internet use is planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online bullying including sexual harassment and peer on peer abuse

Online Safety Group

The Online Safety Group provides a consultative group 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 Governing Body.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Co-ordinator with:

- The production / review / monitoring of the school Online Safety Policy / documents.
- The monitoring of the school filtering protocols
- Monitoring network / internet / incident logs
- Consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- Monitoring improvement actions identified Pupils
- Are responsible for using the school digital technology systems in accordance with the class rules
- Will know and understand expectations on the use of mobile devices, digital cameras and class ipads.
- Will know and understand expectations on the taking / use of images and online bullying.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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 play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and on-line pupil records
- Their children's personal devices in the school (where this is allowed)
- Responsible for ensuring their child is accessing home learning in a safe manor

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the rules around e- safety. They should be encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices

- In lessons where internet use is planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical support provider (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Education – Parents / Carers

Parents/carers play an essential role in the education of their children and in the monitoring / regulation of their children's online behaviours. Parents 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:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Direct discussions with class teacher
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / 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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- 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 Co-ordinator (or other nominated person) will review guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in a staff meeting.

- The Online Safety Co-ordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / 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 / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school 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 will be provided with a username and secure password by Sweethaven or the school, who will keep an up to date record of users and their usernames.
- Users are responsible for the security of their username and password and will be required to change their password regularly.
- The "master / administrator" passwords for the school IT systems, used by the support provider (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- The Admin team 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 changes.
- 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
- Users report any actual / potential technical incident / security breach directly to Sweethaven, and the Online Safety Co-ordinator/ SLT.
- 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 workstations 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, through the use of a "guest" login. Access privileges are minimal.
- 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 (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, laptop or other technology that usually has the capability of utilizing the school's wireless network. The device then has access to the wider internet, which may include cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The AUP should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy and Anti-Bullying Policy. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils and parents / carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes (come to school and locked away for duration of the day given back on their bus)*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Log of devices kept by sweet haven about where technology is allocated. Lisa has a log of school allocated phones.

School owned / provided devices:

- Who they will be allocated to
- Where, when and how their use is allowed – times / places / in school / out of school
- If personal use is allowed
- Levels of access to networks / internet (as above)
- Management of devices / installation of apps / changing of settings / monitoring
- Network / broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking / storage / use of images
- Exit processes – what happens to devices / software / apps / stored data if user leaves the school
- Liability for damage
- Staff training
- Laptops can be taken home to continue work from home
- Ipads to remain at school not be taken off school premises as these are not secure

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff / pupils / students / visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks / internet (as above)
- Network / broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search users devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.
- Taking / storage / use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification / labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes.

Use of digital and video images

Home learning

Evisense

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 / academy 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 i.e. using Evisense within the parental consent parameters set by the Evisense leaders. Those images should only be taken on school equipment; the personal equipment of staff should never be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others.
- Photographs published on the website will be used with parental permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. This is detailed in the Data Protection policy.

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	Not allowed
Mobile phones may be brought to the school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones / cameras								
Use of school ipads								
Use of personal email addresses in school or on school network								
Use of school / academy email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

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

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the DSL, 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 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.
- Personal information should not be posted on the school website and only official email addresses be used to identify members of staff.

Social Media - Protecting Professional Identity

There is an increase in use of social media for professional and personal purposes, alongside this there is clear guidance for staff to manage risk and behaviour online is essential. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'.

All schools 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 liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through the following;

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

School staff should ensure that:

- No reference should be made in social media to pupils, parents/ carers, school staff or the school name
- 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- It is advised by Gosden that staff not use their full name on social media – to minimise the risk of students and parents/carers attempting to contact them via social media.

If Gosden decide to establish a 'school social media' account there will 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
- We would also create a guidance document for parents outlining how the account is designed to be used
- A code of behaviour for users of the accounts, including
    - 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 personal social media accounts. In all cases, where a personal account is used which associates itself with the school or

impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer.

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Dealing with unsuitable / inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material, is illegal and is banned from school and all other technical systems. Other activities, e.g. cyber-bullying, will 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	

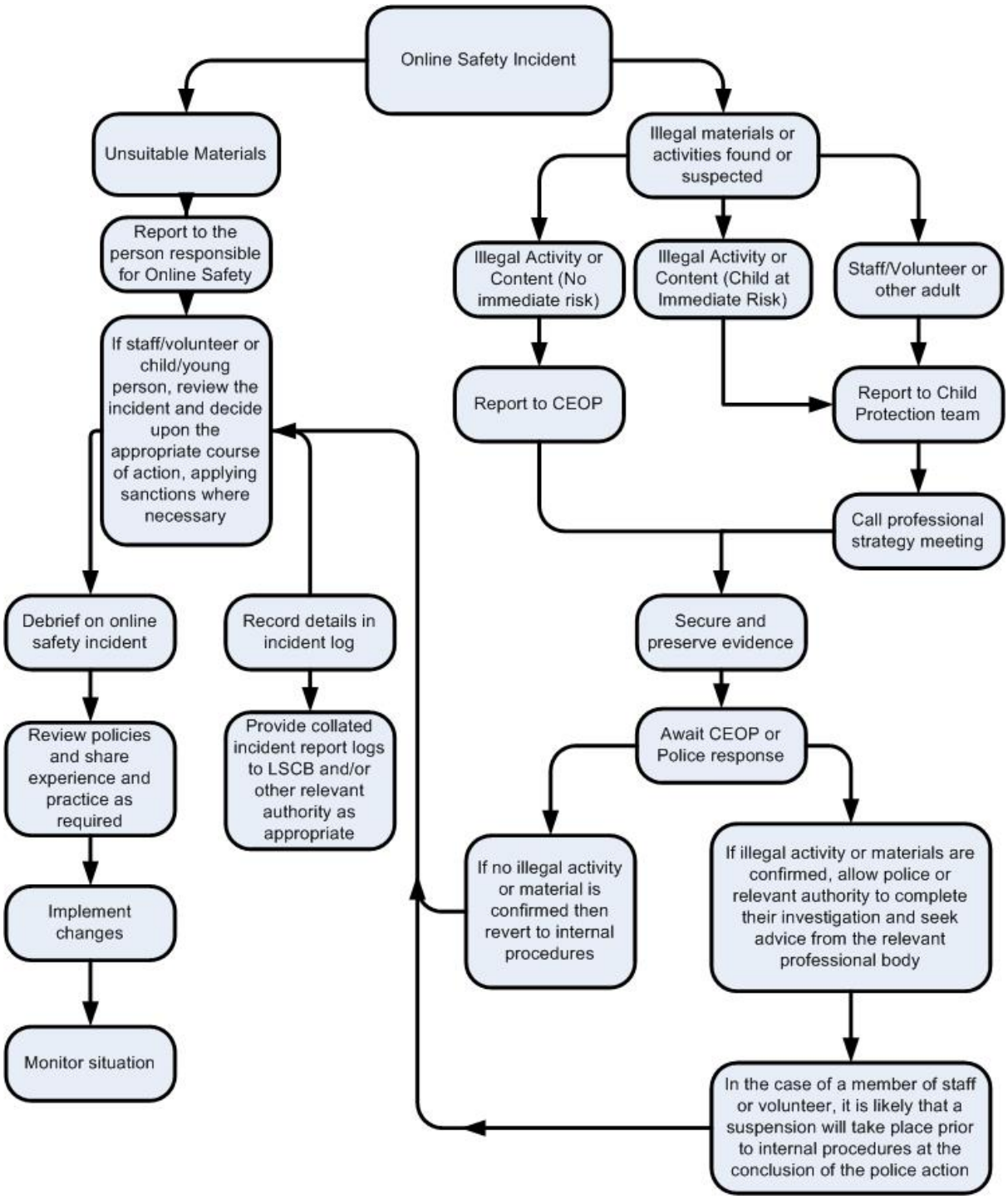
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other 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)						
On-line gaming (non-educational)						
On-line gambling						
On-line shopping / commerce						
File sharing						
Use of social media						
Use of messaging apps						
Use of video broadcasting e.g. Youtube						

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).

Illegal Incidents

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.



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 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
    - 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* and 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.

School Actions & Sanctions

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 / tutor	Refer to Head of Department / Year /	Refer to Headteacher / Principal	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 eg 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									
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device									
Unauthorised / inappropriate use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school / academy network by sharing username and passwords									
Attempting to access or accessing the school / academy network, using another student's / pupil's account									
Attempting to access or accessing the school / academy network, using the account of a member of staff									
Corrupting or destroying the data of other users									

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's / academy's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

	Actions / Sanctions							
Staff Incidents	Refer to line managerr	Refer to Headteacher	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								
Unauthorised downloading or uploading of files								
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								
Careless use of personal data e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature								

Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy								
Using proxy sites or other means to subvert the school's / academy's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone.

This Acceptable Use Agreement is intended to ensure:

- That staff agree how to use the internet safely and responsibly when at Gosden house school and at home

Staff (and Volunteer) Acceptable Use Policy Agreement

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 Gosden House 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.

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 Gosden House 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) 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 intended for educational use and that I will not use the school system for personal use
- 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.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the DSL.

I will be professional in my communications and actions when using Gosden House ICT 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.
- Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites on my own personal device (i.e. phone) on my break in the staff room with no children present
- 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.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted.
- I will ensure that my data is regularly backed up and use staff share to keep files secure
- 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 install or attempt to install programmes of any type on a machine unless approved and completed by Sweethaven.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- 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 to disclose such information to an appropriate authority i.e. sharing information on CPOMS.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

SIGN OFF

I understand that I am responsible for my actions in and out of Gosden House School:

- I understand that this Acceptable Use Policy applies not only to my work and use of Gosden House digital technology equipment in school, but also applies to my use of my personal equipment on the premises or in situations related to my employment by the school / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above 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: .....

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Members of staff may use digital cameras to record evidence of activities in lessons and out of school.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publically shared by any means parents will have given permission. Parents will be given a permission form to sign consenting to using their children's images on Evisense, the school website and on media respectively. These permissions will be shared with relevant staff and kept up to date by the school office.

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

Parents/carers are allowed to take pictures of their children at a school play or assembly in a communal area i.e. the hall. They are not allowed to use their mobile phones in classrooms at all. Parents/carers can not take pictures of children other than their own and they **must never** upload pictures they have taken to social media.