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 last review	Charlotte Almond June 2025
Next review date	Summer 2026
Date approved and signed in governing body meeting	
Signed - Chair of Governors	**Signed - Head teacher** *Rebecca Smale*

Table of Contents

Development / Monitoring / Review of this Policy

A working group made up of has developed this Online Safety policy

- Deputy head teacher
- Online Safety Co-ordinator
- Sweethaven (IT service provider)

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	*Monday 30 June 2025*
The implementation of this Online Safety policy will be monitored by the:	*Senior Leadership Team*
Monitoring will take place at regular intervals:	*Spring term annually*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Autumn term annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*June 2025* *Reviewed September 2025*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Area Schools' Officer, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering, using Senso.
- The annual PSHE student survey will include questions around e – safety relevant to our students

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 where needed. 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 and where known will 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
- ensure the school has appropriate filtering and monitoring systems in place and regularly review their effectiveness
- ensure that the leadership team and staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when they are identified

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 DSLs and Online Safety co-ordinator.
- 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 support those colleagues. Supervision is available.
- 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. Sweethaven, to discuss technical support and updates i.e. filters.
- To carry out an annual risk assessment via pupil survey that considers and reflects the risks that the pupils face.
- To be aware of, attend training on, and guide students and staff on the risks and ethical impact of Artificail Intelligence (AI).
- To monitor and support individuals on the Online safety student watch list at least termly.

Technical staff – Sweethaven

The Network Manager is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required online safety technical requirements
- Users may only access the networks and devices through a properly enforced password protection in which passwords are sufficiently robust and meet guidance around password strength.
- A cyber security and GDPR review is conducted on behalf of the school
- A security audit is conducted on behalf of the school annually
- 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.
- Sweethaven will provide training and advice to school staff so that they can be responsible for monitoring use of the network/internet using Senso
- Implementing and updating software/school systems 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' (refer to Appendix 1)
- They report any suspected misuse or problem to the DSL.
- All digital communications with pupils and parents/carers is on a professional level and only carried out using official school systems.
- Online safety is 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.
- Ensure effectiveness of filtering systems through routine use and alert Sweethaven of any abnormalities that occur i.e. illicit websites or filtering not applying.
- Students' 'digital passports' are up to date and reviewed annually.

Designated Safeguarding Leads

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 child on child abuse
- Artificial Intelligence
- Sharing of nude and semi-nudes

Online Safety Group

The Online Safety Group provides a consultative group with responsibility for issues regarding online safety and the monitoring of the online safety policy, including the impact of initiatives. The group will also be responsible for reporting to the Governing Body. Gosden House School Online Safety Group includes Emily Mainwaring (Deputy Head), Rebecca Smale (Head Teacher), Beth Sutton (Child and Family Support Worker), Charlotte Almond (Online Safety Co-ordinator), Karen Harris (Business Manager), a representative from Sweethaven and Helen Johns (Safeguarding Governor).

Members of the Online Safety Group will assist the Online Safety Co-ordinator with

- The production/ review/ monitoring of the school Online Safety Policy.
- 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 identified improvement actions.

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.
- Contributing to and updating Digital Passports annually.

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. 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 Current Parent Resources sections of the website and on-line pupil records.
- Their children's personal devices in the school (where this is allowed).
- Responsibility for ensuring their child is accessing home learning in a safe manner.
- Supporting students in contributing to and updating Digital Passports annually.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, we will also educate pupils in how to use the internet safely. The education of pupils in online safety is 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. They need to know where they can go for support and how to treat one another online.

Online safety should be a focus in PSHE particularly 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. This will be provided in the following ways:

- A planned online safety curriculum should be provided as part of PHSE lessons and should be regularly revisited.
- Pupils should be taught to be critically aware of the materials/ content they access online and be taught to validate the accuracy of information.
- 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 Online Safety Co-ordinator and then Sweethaven 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.

The updated Keeping Children Safe in Education (KCSIE) guidance for 2025 emphasises the importance of protecting students from online harms, including misinformation and disinformation.

Misinformation refers to false or inaccurate information that is spread without the intention of causing harm. This can include:

Unintentional errors: Mistakes or misunderstandings that are shared online.

Outdated information: Old information that is no longer relevant or accurate.

Misleading information: Information that is presented in a way that is misleading or deceptive, but not necessarily with malicious intent.

Disinformation, on the other hand, refers to false or inaccurate information that is spread with the intention of causing harm or manipulating people's beliefs or actions. This can include:

Propaganda: Biased or misleading information that is spread to promote a particular ideology or agenda.

Fake news: False or fabricated information that is presented as factual news.

Manipulated media: Altered or fabricated images, videos, or audio recordings that are designed to deceive or manipulate people.

Both misinformation and disinformation can have serious consequences, including:

- Undermining trust in institutions: Spreading false information can erode trust in institutions, such as government, media, or education.
- Influencing public opinion: Misinformation and disinformation can shape public opinion and influence people's decisions.
- Causing harm to individuals: False information can cause harm to individuals, such as damage to their reputation or well-being

To address this the school will;

- Continue to implement robust Filtering and Monitoring Systems: Ensure that online safety provisions are regularly reviewed and updated to prevent students from accessing harmful content.

- Continue to provide a strong Online Safety curriculum which supports students in how to critically evaluate online information, identify potential threats and develop an understanding that not everything online is accurate or trustworthy.

- Continue to work with parents and staff to promote a cohesive approach to online safety and ensure everyone is aware of the potential risks and signs of harm.

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
- Newsletter
- School website
- Parentmail
- Parents/Carers evenings
- High profile events/ campaigns e.g. Safer Internet Day
- Direct discussions with class teacher
- Direct discussions with Online Safety Co-ordinator
- Digital Passports

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:

- 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 will receive updates through network emails and 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 will provide advice/guidance 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 the online safety team. This could be through:

- 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 Security

Technical – infrastructure/ equipment, filtering, monitoring and passwords

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.
- Sweethaven complete an annual security audit and give recommendations to be reviewed.
- 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.
- The "master / administrator" passwords for the school IT systems, used by the Sweethaven must also be available to the Head teacher. These are stored securely in Sweethaven systems, if they are needed the Head teacher is able to call Sweethaven and access these. Sweethaven will then audit who has accessed them and when.

- Sweethaven 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. Sweethaven have implemented Senso to allow school to monitor student activity via key words.
- There is a network security device on the front end of the network (called SonicWALL) for network filtering - updates to list and key words are applied at the request of the school.
- As per the 'Counter Terrorism Securities Act 2015', schools are required to ensure that children are safe from terrorist and extremist material on the internet. This is ensured through secure filtering and monitoring software managed by Sweethaven.
- The school has provided enhanced/ differentiated user-level filtering.
- Users report any actual/ potential technical incidents/ security breaches directly to Sweethaven, the Online Safety Co-ordinator or 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. The school infrastructure and individual workstations are protected by up to date virus software.
- There is provision for temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems, with a "guest" login. Access privileges are minimal.
- Memory sticks are only to be used if they are encrypted. Otherwise, staff are able to use one drive and staff share to access the documents they need.

Staff Passwords

- All staff users will be provided with a username and password by Debby Brown who will keep an up to date record of users and their usernames.
- The account should be "locked out" following six successive incorrect log-on attempts.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Users are responsible for the security of their username and password.

Student / Pupil Passwords

- Pupils have their own log-ins for *Teams, Education City and Bug Club* accounts that they are able to use in school and at home for home learning. Passwords are set and then changed by parents and students. Debby keeps a log of children's usernames.

Training / Awareness

Members of staff will be made aware of the school's password guidance:

- at induction
- through the school's online safety policy

Mobile Technologies

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 utilising 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 devices in a school context is educational. The 'Acceptable Use Policy' should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy.

Some members of staff at Gosden House School have school allocated phones in order to contact staff or parents. The safe use of these is outlined in the Acceptable Use Agreements.

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 (to be locked away and only used at staff allocated break times in staff areas i.e. staffroom)	Yes (to be locked away in the office and returned at end of visit)
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	Yes (guest Wi – Fi)	Yes (guest Wi-Fi)
Network access	Yes	Yes	Yes	No	No	No

Admin staff have a log of all Gosden House School devices including staff laptops and school issued mobiles on the Asset Register.

School owned / provided devices:

- School iPads remain in school.
- School issued laptops are allowed to be taken home to continue work from home (they each have password protection).
- Levels of access to networks/ internet (as above).
- Management of devices/ installation of apps can only be done by Sweethaven when authorised.
- Technical support is provided by Sweethaven who are emailed with any technical issues or requests.
- Filtering of devices is done and monitored by the network set up.
- Taking/ storage/ use of images – photos are taken on school iPads and these are kept in school. Photos may be on 'in school' computers in order to upload to Evisense but are kept on password-protected devices.

[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.

- Staff are aware that they must lock their computers when they are away from them.

Personal devices:

- Staff are only allowed to use personal mobile devices at school when on their break in an adult designated area, e.g. the staffroom or PPA office, and their device should be locked away the rest of the time.
- Storage of devices for visitors is locked in the school office.
- Storage of devices for staff is in a locked cupboard in the school office or staffroom.
- Levels of access to networks / internet (as above).
- Personal mobile devices are able to link to 'Guest Wi- FI' system
- No technical support is available for personal devices.
- The police have the right to take, examine and search users' personal devices in the case of misuse (England only).
- No images are permitted to be taken on personal devices.
- Visitors will be informed of school requirements by the office staff when they arrive.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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, Evisense, school newsletter or 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 only 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 protection, these images must 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 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:

Communication Technologies	Staff & other adults			Students / Pupils				
	Allowed	Allowed at certain times	Not allowed	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		✓		✓				

As detailed above staff are only allowed to use personal mobile devices on their break in adult areas i.e. staff room and will be linked to the 'Guest Wi- Fi' and therefore will not have gull network access on their personal devices.

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' and the schools' Code of Conduct.

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 House 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.

Personal Use:

- 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 those 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 (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

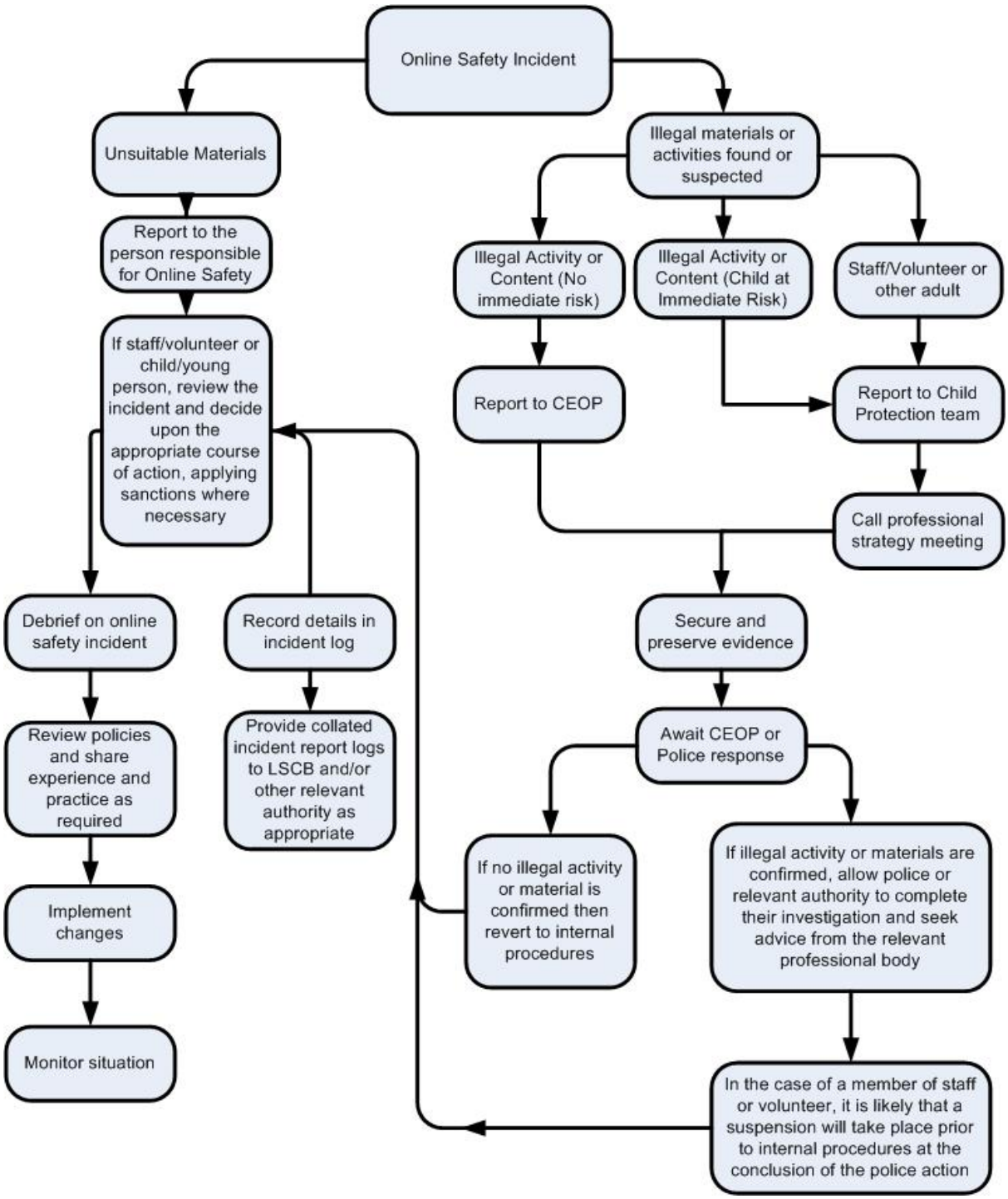
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational) i.e. phonics games	X				
On-line gaming (non-educational) i.e. CBeebies' games		X			
On-line gambling				X	
On-line shopping/commerce acceptable for school orders etc.	X				
File sharing (only on staff share and one drive)		X			
Use of social media (only acceptable by staff on break in adult only areas i.e. staff room and only on personal devices and not using school internet network)		X			
Use of messaging apps (only acceptable by staff on break in adult only areas i.e. staff room and only on personal devices and not using school internet network)		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).

Illegal Incidents

If there is any suspicion that the website(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 disciplinary 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	Refer to DSL	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	Record on CPOMS	Sanction e.g. detention / exclusion (include education around possible incident)
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X				X		X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X			X		X	X
Unauthorised/ inappropriate use of social media /messaging apps/personal email	X	X	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X		X	X	X	X	X
Allowing others to access school/academy network by sharing username and passwords	X	X	X	X		X	X	X	X
Attempting to access or accessing the school network, using another student's / pupil's account	x	x	x			x		x	x

Attempting to access or accessing the school network, using the account of a member of staff	x	x	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		x	x		x	x
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Head teacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Sweethaven Staff for action re filtering etc.	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	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using a another person's account	X	X	X		X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	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		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system								
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	x

Appendix 1

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 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 will store passwords securely.
- 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. This will be on my phone's network or using 'Guest Wi- Fi'.
- I will only communicate with 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 staffshare 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 (including apps).

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or 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, e.g. sharing information on CPOMS.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- If I am issued with a school mobile phone this is to be used for professional purposes only i.e. sickness line or home/school worker contacting families. I will not use this device for any private means.

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.
- 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: .....

Appendix 2

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 or iPads to record evidence of activities in lessons and out of school.

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.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Any media that has been shared on the school website, in the school newsletter or in local press will have been done so with parental consent. Levels of parental consent for each child is stored in the photographic permission document. Teachers can refer back to this to check photographic permissions for each child so they are able to add images to the school newsletter or share on Evisense correctly and within these parameters.

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. Parents/ carers cannot take pictures of children other than their own and they **must never** upload pictures they have taken to social media in order to protect other children who may be in the background of images.

Appendix 3

Gosden House School Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy.
- Logs are maintained of access by users and of their actions while using the system.
- There is effective guidance and training for users.
- There are regular reviews and audits of the safety and security of school computer systems.
- There is oversight from senior leaders and these have impact on policy and practice.

Gosden House has a managed ICT service provided by an outside contractor – Sweethaven. Gosden recognises it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures needed. Gosden house will share the most up to date Online Safety Policy and Acceptable Use Agreements with Sweethaven.

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

Responsibilities

Sweethaven, SLT and the Online Safety Co-ordinator, will hold the responsibility for the management of the school's filtering. They will manage the school filtering and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be reported to and authorised by a second responsible person prior to changes being made.

All users have a responsibility to report immediately to online-safety co-ordinator and Sweethaven any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. This should be recorded on CPOMS as well.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/ security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Personal mobile devices are not allowed access to the school's internet network. The school maintains and supports the managed filtering service provided by Sweethaven.

Education / Training / Awareness

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Changes to the Filtering System

If a teacher would like to request changes to the filtering system i.e. to reach an educational site that is currently blocked, they must contact the head teacher or school business manager for approval and then once this is gained one of the account managers can contact Sweethaven to request this change.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered should report this on CPOMS and SLT will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Sweethaven
- Online safety group

The filtering service will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance

Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*" (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in 2022. Amongst the proposed changes, schools will be obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.*"

In response UKSIC produced guidance on – information on "Appropriate Filtering"

NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/

Appendix 4

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

The use of mobile technologies brings both real benefits and challenges for the whole school community, including teachers, and the only effective way for a school to implement these successfully is to involve the whole school community from the outset.

- 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 and allocated to a single user	**School owned for use by multiple users**	**Authorised device[2]**	**Pupil/Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	**Yes**	**Yes**	**Yes**	Yes (but kept locked away until end of day so student can have them on transport)	Yes (but locked in cupboard and only used during day in break times in child free area i.e. staff room)	Yes (but locked in reception during visit)
Full network access	***Yes***	***Yes***	***Yes***	**No**	**No**	**No**
Internet only	**-**	**-**	**-**	**No**	**Yes**	**Yes**
No network access	**-**	**-**	**-**	**Yes**	**Yes**	**Yes**

- **The school has provided technical solutions for the safe use of mobile technology for school devices/ personal devices:**
    - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted.
    - All school devices are subject to monitoring.
    - Pro-active monitoring has been implemented to monitor activity by Sweethaven.
- *When personal devices are permitted:*
    - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access.
    - Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and

[2] 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

their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.

- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.

- **Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;**
  - Devices may not be used in tests or exams.
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements.
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in school. Chargers must be PAT compliant.
  - Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately. This must be done on school devices only not personal devices.
  - Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances.

Appendix 5

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Gosden House School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/ carers and pupils are actively encouraged to find creative ways to use social media safely and at home. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by staff, parents, carers and children.

Scope

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/ or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

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 affects the school, 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.

Organisational control

Roles & Responsibilities

- **SLT**
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy.
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- **Staff**
    - Attending appropriate training.
    - Not naming the school on personal accounts.

Process for creating new accounts

Gosden House School does not have any social media accounts and will not create one. We will continue to use the school website, the newsletter and our Parentmail as our main online communications. 'Class List' is used as a parent networking site and is overseen by the school.

Gosden parents are able to use 'Class List' an app used for parental communication. Parents are made aware of the code of conduct (appendix 8) and privacy notice of 'Class List'. Although the school do not manage 'Class List' we are able to monitor use and the school reserves the right to delete any inappropriate or offensive content. The school is not responsible for communication of individuals on 'Class List'.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the

matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media account. 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. 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.
    - The school permits reasonable and appropriate access to private social media sites on your own personal device, within your break time and in a child free zone i.e. staff room. You should not use the school Wi-Fi for this.
- **Pupil**
    - **Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.**
    - The school's education programme should enable the pupils to be safe and responsible users of social media.
    - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy.
- **Parents/ Carers**
    - **If parents/ carers have access to a school learning platform where posting or commenting is enabled, parents/ carers will be informed about acceptable use i.e. on Evisense and Classlist.**
    - Parents/ Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/ carer to remove the post and invite them to

discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- 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.

Managing your personal use of Social Media:

- "Nothing" on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

Appendix 6

Gosden House School – Online Safety Team Terms of Reference

1. Purpose

To provide 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.

2. Membership

2.1. The online safety group will seek to include representation from a range of stakeholders.

The composition of the group includes -

- SLT member (DSL) – Cindy O Sullivan
- Teaching staff member – Charlotte Almond
- Online Safety Co-ordinator – Charlotte Almond
- Governor – Pat Adams
- ICT Technical Support staff - Sweethaven representative
- School Business Manager – Karen Harris

2.2. Other people may be invited to attend the meetings at the request of the team on behalf of the committee to provide advice and assistance where necessary.

2.3. Team members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Team members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying team members;
- Inviting other people to attend meetings when required by the team;
- Guiding the meeting according to the agenda and time available;

- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.
- The Chairperson of the Gosden House Online – Safety team is Charlotte Almond

4. Duration of Meetings

Meetings shall be held annually. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead with the following:

- To keep up to date with new developments in the area of online safety
- To annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/ or developments in the area of online safety
- Surveys/questionnaires for pupils, parents/carers and staff
- Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the school (Sweethaven)
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites – Sweethaven)
- To monitor incidents involving cyberbullying for staff and pupils.

Acknowledgement

This template terms of reference document are based on one provided to schools by Somerset County Council

Appendix 7

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individuals' data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if

their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial;
- The right to respect for private and family life, home and correspondence;
- Freedom of thought, conscience and religion;
- Freedom of expression;
- Freedom of assembly;
- Prohibition of discrimination;
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/ carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

Appendix 8

Links to other organisations or documents

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/
Periodic table of sinister emojis-
https://www.worklifecentral.com/SiteAssets/Files/Emojis%20Periodic%20Table.pdf

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour -
http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign
https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Digital Literacy & Citizenship curriculum
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection

360data - free questionnaire and data protection self-review tool
ICO Guide for Organisations (general information about Data Protection)
ICO Guides for Education (wide range of sector specific guides)
DfE advice on Cloud software services and the Data Protection Act
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Computing
ICO - Guidance we gave to schools - September 2012
IRMS - Records Management Toolkit for Schools
NHS - Caldicott Principles (information that must be released)
ICO Guidance on taking photos in schools
Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

UKSIC – Appropriate Filtering and Monitoring
Somerset - Questions for Technical Support
NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents' workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - it's not chalk and talk anymore!"
Ofcom –Media Literacy Research

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.