GODOLPHIN

Online Safety Policy

Reviewed in: September 2022
Review in: September 2023
Reviewed by: Senior Deputy Head, Director of Digital Strategy, Head.

Refer also to the following policies/documents:

Online Safety 2. Acceptable Use Policy Agreements
Online Safety 3. Technical Security Policy
Online Safety 4. Data Protection Policy (incorporating Personal Data Handling)
Online Safety 5. Social Media Code of Practice
Online Safety 6. Online Safety Committee Terms of Reference
Online Safety 7. Use of Digital and Video Images Agreement
Online Safety 8. Use of Cloud Systems Permission Form
Data Sharing Agreements
Privacy Notices
Search Policy

GODOLPHIN

Table of Contents

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Godolphin School will, through its Online Safety Policy and the implementation of the same, ensure that it meets its statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside the School. This policy also forms part of the School's protection from legal challenge, relating to the use of digital technologies.

Due to the ever-changing nature of digital technologies, the School reviews its Online Safety Policy annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place.

All references in this policy to parents also refer to carers or guardians who have responsibility for pupils at the School.
All references in this policy to pupils also refer to pupils as members of the whole School community.

Schedule for Review

The implementation of this Online Safety Policy will be monitored by:	The DSL and the Deputy Head Pastoral: Online Safety Coordinators
Monitoring will take place :	Annually during the first half of the Autumn Term
The Governors Governance Committee will receive a report on the implementation of the Online Safety Policy :	Annually during the Summer Term
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:	Summer 2022
Should serious online safety incidents take place, the following person should be informed who will contact the relevant external persons/agencies as appropriate:	Richard Dain, Senior Deputy Head, Designated Safeguarding Lead

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:
    - pupils (together with parents where appropriate)
    - staff

Scope of the Policy

This policy applies to all members of the Godolphin School (including pupils, staff, volunteers, parents, visitors and community users) who have access to and are users of School ICT systems, both in and out of the School.

The Education and Inspections Act 2006 empowers Heads, 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 are linked to membership of the School. The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the School's *Behaviour and Discipline Policy* and *Living Together at Godolphin: anti-bullying*.

The School will deal with such incidents within this policy together with associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of School.

Legislation

There are a number of Acts which form the legislative framework under which the School's Online Safety policies and guidance have 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.

Further details of the legislation relevant to the Online Safety policies can be found in Appendix 1.

Related Policies

This policy document refers to other Online Safety policies and documents, namely:

- Online Safety 2. Acceptable Use Policy Agreements
- Online Safety 3. Technical Security Policy
- Online Safety 4. Data Protection Policy (incorporating Personal Data Handling)
- Online Safety 6. Online Safety Committee Terms of Reference
- Online Safety 7. Use of Digital and Video Images Agreement
- Online Safety 8. Use of Cloud Systems Permission Form
- Online Safety 9. Privacy Notices (incorporated in Data Protection Policy)
- Online Safety 10. Electronic Devices - Searching and Deletion

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. This will be carried out by the Governors' Governance Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor and sits on the Online Safety Committee.

The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Co-ordinator
- Attendance at Online Safety Committee meetings
- Regular monitoring of Online Safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors 'committee/meetings

Head and SMT

- The Head has a duty of care for ensuring the safety (including Online Safety) of members of the School community, although the day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.
- The Head and designated members of the Senior Management Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Online Safety Coordinators

- Lead the Online Safety Committee
- Take day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the School's Online Safety policies/documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- Provide training, access to training and advice for staff
- Liaise with the local authority/relevant body
- Liaise with IT system technical staff
- Receive reports of Online Safety incidents and create a log of incidents to inform future Online Safety developments
- Meet regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attend relevant meetings /committee of Governors
- Report regularly to SMT

Director of Digital Strategy

The Director of Digital Strategy, often through the contracted service company for maintenance and monitoring of the IT systems, is responsible for ensuring that:

- The School's technical infrastructure is secure and is not open to misuse or malicious attack
- The infrastructure incorporates effective anti-virus protection
- The School meets required Online Safety technical requirements
- Users may only access the networks and devices through a properly enforced password protection policy, 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
- They keep up to date with Online Safety technical information in order to carry out their Online Safety role effectively and to inform and update others as relevant
- The use of the network/Internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Coordinator and designated members of SMT for investigation/action/sanction.
- Monitoring software/systems are implemented and updated as agreed in School policies

Teaching and Support Staff

All 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 will

- have read, understood and signed the Online Safety Staff and Volunteers Acceptable Use Policy Agreement
- report any suspected misuse or problem to the Online Safety Coordinator and designated members of SMT for investigation/ action/ sanction
- maintain digital communications with pupils/pupils/parents on a professional level and only carried out using official School systems
- embed Online Safety practices in all aspects of the curriculum and other activities
- help pupils/pupils understand and follow the Online Safety and Acceptable Use Policies
- ensure Pupils/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other School activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, guide pupils to sites checked as suitable for their use and ensure that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Lead for Child Protection/Safeguarding

The DSL will be responsible for oversight of safety in the School, trained in Online Safety issues and be aware of the potential for serious child protection or safeguarding issues arising, for example, from:

- Sharing of personal data
- Access to illegal/ inappropriate materials or inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Online bullying

Online Safety Committee

The Online Safety Committee provides a consultative group that has wide representation from the School community, with responsibility for issues regarding Online Safety and the monitoring of the Online Safety policy including the impact of initiatives.

Members of the Online Safety Committee will assist the Online Safety Coordinator with:

- the production/review/monitoring of the School Online Safety policy/documents.
- the production/review/monitoring of the School filtering policy and requests for filtering changes.
- mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents[/carers] and the pupils/pupils about the Online Safety provision

Pupils

All pupils:

- are responsible for using the School digital technology systems in accordance with the Online Safety Pupil/Pupil Acceptable Use Policies
- acknowledge their agreement with the terms and conditions of the Acceptable Use Policy on entry to the School and at the cross-over of each phase. This might be at the end of one academic year or the beginning of the next. The phases are:
    - On entry to Reception up to Year 3
    - Between Year 4 in Prep to Second Year in Senior School
    - Between Third Year and Fifth Year
    - Sixth Form
- Seek to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras.
- are expected to understand policies on the taking/use of images and on online bullying and to behave in a responsible manner at all times
- 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 Policies cover their actions outside School

Parents

Parents 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 opportunities to help parents understand these issues through parents' evenings, weekly communications, the School website and information about national/local Online Safety campaigns/literature. Parents of younger girls will be asked to support the School in its work by counter-signing an Acceptable Use Agreement.

Parents 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/portals and on-line pupil records
- their children's personal devices in the School

Community Users

Community Users who access School systems/website/VLE as part of the wider School provision will be expected to sign a Community User Online Safety Acceptable Use Agreement before being provided with access to School systems

Policy Statements
Education and Training

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 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 is a focus in all areas of the curriculum and staff are required to reinforce Online Safety messages across the curriculum. The Online Safety curriculum is broad and relevant and provides progression, with opportunities for creative activities. It is provided in the following ways:

- A planned Online Safety curriculum forms part of Computing/PSHCEE/other lessons and is regularly revisited
- Key Online Safety messages are reinforced as part of a planned programme of prayers and tutorial/pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will 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 will be helped to understand the need for the pupil/pupil Online Safety Acceptable Use Agreements and encouraged to adopt safe and responsible use both within and outside School
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, pupils will be guided to sites checked as suitable for their use and processes will be in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff will 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, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that ICT Services temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be emailed as an IT Ticket to ICTSupport@gododolphin.org, with clear reasons for the need. Action taken will be noted in the 'Filtering/Change Control Log' available in 'Online Safety 3. School Technical Security Policy'.

Parents

Many parents have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line 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 through:

- Curriculum activities
- Letters, newsletters, School website
- Parents evenings/sessions
- High profile events/campaigns eg Safer Internet Day
- Reference to the relevant web sites

The Wider Community

The School may provide opportunities for local community groups/members of the community to gain from the School's Online Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and Online Safety
- Online Safety messages targeted towards grandparents and other relatives as well as parents.
- The School website providing Online Safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth/ sports/ voluntary groups to enhance their Online Safety provision

Staff and Volunteers

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

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the staff development process.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the School Online Safety policies and Acceptable Use Agreements.
- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

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

Governors

Governors will be offered Online Safety training/awareness sessions, with particular importance for Governors who are members of any committee/group involved in technology/Online Safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association /or other relevant organisation (eg SWGfL or Smoothwall).
- Participation in School training/information sessions for staff, parents or governors: this may include attendance at assemblies/lessons.

Technical Security

The School is responsible for ensuring that the School infrastructure/network is as safe and secure as is reasonably possible, that policies and procedures approved are implemented, and that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities. The Online Technical Security Policy provides detailed guidance on the School's responsibilities and on good practice and covers:

- Password security
- Cloud services
- Data backup
- Filtering and monitoring

Data Protection Policy (incorporating Personal Data Handling)

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The School's Data Protection Policy (incorporating Personal Data Handling) provides detailed guidance on the School's responsibilities and on good practice.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the School considers the following as good practice:

- The official School email service may be regarded as safe and secure and is monitored
- Users must immediately report, to the nominated person, in accordance with the School behaviour policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents (email, social media, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging or social media must not be used for these communications
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual School email addresses for educational use
- Pupils are taught about Online Safety issues, such as the risks attached to the sharing of personal details. This also includes strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff and pupils.

The table below outlines the School's attitudes and approach to these technologies:

	Staff & other adults				Pupils/Pupils			
Communication Technologies	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to School		X				X	X	X
Use of mobile phones in lessons			X					X
Use of mobile phones in social time		X					X	
Taking photos on mobile phones/cameras			X					X
Use of other mobile devices e.g. tablets, gaming devices			X					X
Use of personal email addresses in School, or on School network (for personal business only)		X				X		
Use of School email for personal emails	X							X
Use of messaging apps		X					X	X
Use of social media		X					X	X
Use of blogs		X					X	X

Mobile Technologies

Mobile technology devices may be a School owned/provided or privately-owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the School's wireless network. The device then has access to the wider internet which may include social media, our learning platform, and other cloud based services such as email and data storage.

The School provides technical solutions for the safe use of mobile technology for both School devices and personal devices. This solution relies on wireless connection to the School's ICT infrastructure:

- All School owned devices are controlled though the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices connected to the network according to the level and requirements of the user
- The School addresses broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by use of personal mobile devices
- Filtering and monitoring is applied for all mobile technologies connected to the network and attempts to bypass this are not permitted
- 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 their parents) 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 any device due to changes made to the device while on the School network or whilst resolving any connectivity issues
- The School recommends that devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the School.
- Users have an obligation to set pass-codes or PINs on mobile devices to aid security
- The School is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition recognise that:

- The primary purpose of having a personal device at School is educational and this is irrespective of whether the device is School owned/provided or personally owned.
    - Devices may not be used in tests or exams, unless expressly specified, eg by the Special Educational Needs Coordinator

- Visitors are permitted to use mobile technology in line with local safeguarding arrangements, in particular that Digital Images may not be taken in the Prep and EYFS settings
- Users are responsible for keeping their device up to date through software, security and app updates.
- The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in School
- Personal devices should be charged before being brought to School
- Devices must be in silent mode on the School site and on School buses
- School devices are provided to support learning. It is expected that pupils will bring devices to School as required. From September 2021, all students from the First Year to the Fifth Year will be using SurfacePros managed by the School. The Sixth Form will be asked to bring their own laptop or tablet to school for academic purposes
- Confiscation and searching: The School has the right to take, examine and search any device when unauthorised use, either technical or inappropriate, is suspected
- The changing of settings on School owned devices (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- The software/apps originally installed by the School must remain on the School owned device in usable condition and be easily accessible at all times. From time to time the School may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The School will ensure that School devices contain the necessary apps for School work. Apps added by the School will remain the property of the School and will not be accessible to pupils on authorised devices once they leave the School roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- 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
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- Teaching about the safe and appropriate use of mobile technologies is included in the Online Safety education programme.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act), except in the Prep and EYFS settings where this is not permitted. 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 comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images. Those images should ideally only be taken on School equipment. If staff personal equipment is used, the images should be securely deleted from these devices after 48 hours.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog in association with photographs without consent
- Written permission from parents will be obtained before photographs of pupils are published on the School website/social media/local press
- Pupils' work can only be published with the permission of the pupil and parents

A copy of the Digital/Video Images Agreement is available in Appendix 2.

Social Media

Schools have a duty of care to provide a safe learning environment for pupils and staff, and could be held responsible, indirectly for acts of their employees during their employment. Staff members who harass, cyberbully or discriminate on the grounds of sex, race or disability or who defame a third party may render the School liable to the injured party. User responsibilities regarding the use of social media are covered in the relevant Acceptable Use Policy.

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 limiting access to personal information:

- Ensuring that personal information is not published or shared without consent
- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

The Online Safety Social Media Code of Practice provides detailed guidance on the School's responsibilities and on good practice.

Unsuitable/inappropriate activities

Some internet activity, eg accessing child abuse images or distributing racist material, is illegal and would obviously be banned from School and all other technical systems. Other activities such as online bullying are banned and could lead to criminal prosecution. There is, 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 School or outside School when using School equipment or systems.

The School policy restricts usage as described in the table on the following page (page 13).

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 relevant 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 described in the tables below.

GODOLPHIN

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	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					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)			X			
On-line gaming (non-educational) and on-line gambling					X	
On-line shopping/commerce			X			
File sharing (e.g. torrents, video streaming, music streaming, etc)					X	
Use of social media			X			
Use of messaging apps and video broadcasting e.g. YouTube		X				

GODOLPHIN

Pupils

Note:
Action taken will depend on relative severity of incident and consideration of previous offences

Incident	Referral						Sanctions					
	Teacher / Tutor	Head of Department / Year / House Mistress	ICT Services	Parents / Carers	Head	Police	Confiscation of devices / restricted access to technology	Detention	On Report	Removal of network / Internet access	Internal exclusion	Suspension / Exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)			•	•	•	•						•
Unauthorised use of non-educational sites during lessons or prep	•	•	•				•	•	•			
Unauthorised use of mobile phone/digital camera/other mobile device	•	•	•				•	•	•			
Unauthorised use of social media/personal email	•	•	•				•	•	•			
Unauthorised downloading or uploading of files	•	•	•				•	•	•	•	•	•
Allowing others to access school network by sharing username and passwords	•	•	•	•			•	•	•	•	•	
Attempting to access or accessing the School network, using another pupil's/pupil's account	•	•	•	•					•	•	•	
Attempting to access or accessing the School network, using the account of 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 into disrepute or breach the integrity of the ethos of the School	•	•	•	•	•							•
Using proxy sites or other means to subvert the School'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	•	•	•	•			•	•	•	•		

GODOLPHIN

Staff

Note:
Action taken will depend on relative severity of incident and consideration of previous offences

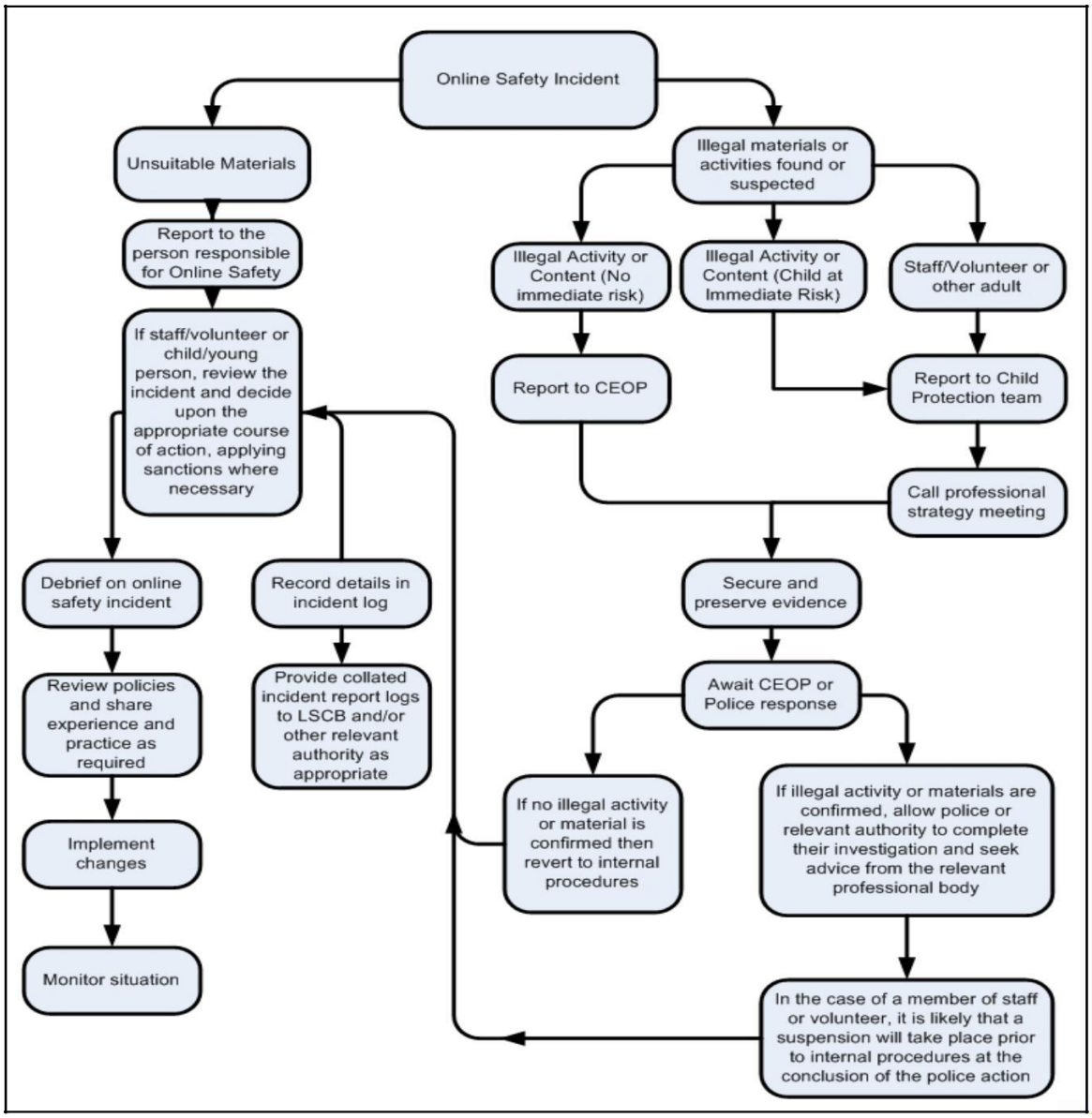
Incident	Action				
	Refer to Line Manger, SIRO, Online Safety Coordinatorasappropriate	Refer to Director of Digital Strategy, ICT Support for action	Refer to Head	Disciplinary Action	Refer to Police, other agencies as appropriate
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	•	•	•	•	•
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 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 and software	•	•	•	•	•
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	•	•	•	•	•
Using personal email/social media/text messaging to carry out digital communications with pupils/pupils	•	•	•	•	•
Actions which could compromise the staff member's professional standing	•	•	•	•	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the School	•	•	•	•	
Using proxy sites or other means to subvert the School'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	•	•	•	•	•

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 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/volunteer 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:
    - o Internal response or discipline procedures
    - o Involvement by national/local organisations (as relevant). o 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:
    - o incidents of 'grooming' behaviour
    - o the sending of obscene materials to a child
    - o adult material which potentially breaches the Obscene Publications Act o criminally racist material
    - o promotion of terrorism or extremism
    - o 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 child protection purposes. The completed forms below should be retained by the group for evidence and reference purposes.

Electronic Devices - Searching & Deletion

Part 2 of the Education Act 2011 (Discipline) allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules. Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

It is essential that all staff are aware of and should implement the School's policy: Online Safety 10: Electronic Devices - Searching and Deletion.

GODOLPHIN

Responding to Incidents of Misuse: Record of reviewing devices/internet sites

Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device *Reason for concern*

Conclusion and Action proposed or taken

GODOLPHIN

Responding to Incidents of Misuse: Report Form

Date	Time	Incident	Action Taken		Incident reported by?	Signature
			What	By Whom		

Appendix 1: Legislation

The following Acts form the legislative framework under which the School Online Safety Policies and guidance have 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.

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 2018

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, specific 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

A person ending 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 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 is 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 she 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 her is guilty of an offence if she knows or ought to know that her 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 a 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

The new 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 a 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

The Act empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils / 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

The above Act extends the powers included in the 2006 Act and gives permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see policy E-Safety 13. Electronic Devices - Searching and Deletion, 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:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Appendix 2: Use of Digital/Video Images Agreement
(Online Safety 7. Use of Digital and Video Images Agreement)

Godolphin Senior School

Use of Digital/Video Images Agreement

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

Images may also be used to celebrate success through their publication in newsletters, on the School website and occasionally in the public media,

The School will comply with the Data Protection Act 2018 and request parents'/carers' permission before taking images of members of the School. The School will also ensure that when images are published the young people cannot be identified by the use of their full names.

In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at School events for their own personal use (as such use in not covered by the Data Protection Act). However, to take images is not permitted in the Prep and EYFS settings. 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 comment on any activities involving other pupils in the digital/video images.

In the New Student Handbook, parents and carers are given clear information as to how their daughter's photograph may be used when they join the School. This is also explained in the Privacy Notice available on the school website. Both documents clearly state how the parent should proceed should they wish their daughter's image not to be used in publications, school social media accounts, or in displays around the school.