



St John's Church of England Primary School

Online Safety Policy

This policy is based on the Southwest Grid for Learning Template as at July 2016

Date Approved:	November 2016
Headteacher:	Mrs Helen Langeveld
Chair of Governors:	Mrs Julie Griffiths
Review Date:	November 2017

Love, Respect, Value

St John's Church of England Primary School is committed to high expectations for all and to embracing equality.

Intentionally blank





Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of: Greg Clough, Helen Langeveld and members of the Watford Girls Grammar School (WGGS) IT Department and in coming months and years we will involve the following as we follow the 360 degree review tool to evolve this policy as the school's infrastructure and pupils ages grow:

- Headteacher / Senior Leaders
- Online Safety Officer
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents and Carers
- Community users

Consultation with the whole school community will now take place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	<i>23 November 2016</i>
The implementation of this Online Safety policy will be monitored by the:	<i>Senior Leadership Team</i>
Monitoring will take place at regular intervals:	<i>Termly</i>
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:	<i>Termly</i>
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:	<i>July 2017</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>Libby Grundy, Safeguarding Governor, Jeremy Hirst, Diocesan Safeguarding Officer, 01727 818107 or 07867 350886 safeguarding@stalbans.anglican.org Hertfordshire, LADO LADO.Referral@hertfordshire.gov.uk or HCC Customer Service Centre 0300 123 4043, Police</i>



The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Surveys / questionnaires of
 - pupils
 - parents / carers
 - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors and community users) who have access to and are users of the school ICT systems and / or wifi, 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 cyber-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 electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school: (In a small school some of the roles described below may be combined, though it is important to ensure that there is sufficient “separation of responsibility” should this be the case).

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 receiving regular information about online safety incidents and monitoring reports. Libby Grundy a member of



the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator (HT and WGGS)
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors' meeting

Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Co-ordinator*.
- The Head Teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant HR disciplinary procedures). [Online Safety BOOST includes an Incident Response Tool that outlines the steps \(and forms to complete\) any staff facing an issue, disclosure or report, need to follow.](#)
- The Head Teacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. [Online Safety BOOST includes access to unlimited online webinar training](#)
- The Head Teacher/ Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
[\[WGGS to work with HT on appropriate monitoring as the school systems and pupil numbers grow and BOOST to provide additional help and support as needed\]](#)
The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:

[\(It is strongly recommended that each school should have a named member of staff with a day to day responsibility for Online Safety, some schools may choose to combine this with the Designated Safeguarding Lead role. Schools may choose to appoint a person with a child](#)



welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school)

In our opening years this role will be split between the HT and WGGs IT team and developed and grown along with the school's systems and pupil numbers supported by the SWGfL resources and the school's IT contractor, Joskos.

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. [Online Safety BOOST](#) includes access to [Whisper](#), an anonymous reporting app that installs onto a school website and extends the schools ability to capture reports from staff, children and parents.
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Technical staff:

(nb. if the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school Online Safety Policy and procedures.)

The Technical Staff are responsible for ensuring:

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required online safety technical requirements and any Online Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**



- the filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person **by ensuring the filter exceptions are reported to and reviewed by the Online Safety Committee at every meeting.**
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the school's ICT systems is regularly monitored **via the RM Dashboard Reporting** in order that any misuse / attempted misuse can be reported to the Head Teacher or Online Safety Coordinator for investigation, action or sanction.

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 Policy (AUP)**
- **they report any suspected misuse or problem to the Head Teacher or Online Safety Coordinator for investigation / action / sanction**
- **all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems**
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained (using Boost) 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



- cyber-bullying

(n.b. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community including pupils and parent / carers, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Coordinator (or other relevant person, as above) with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.



Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices and in the school (where this is allowed)

Community Users

Community Users who access the website / wifi as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school wifi.

Policy Statements

Education – pupils

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

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.



- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and 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 pre-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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's 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 and carers through:

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



Education – The Wider Community

The school will 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 will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, The Ark, The Hub, St John's Playgroup, voluntary groups to enhance their Online Safety provision (supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk)

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. [Online Safety BOOST includes unlimited online webinar training for all, or nominated, staff.](#)
- 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. [Online Safety BOOST includes an array of presentations and resources that can be presented to new staff.](#)
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The Online Safety Coordinator (or other nominated (WGGS) person) will provide advice / guidance / training to individuals as required. [Online Safety BOOST includes an array of presentation resources that the Online Safety coordinator can access to deliver to staff \(<https://boost.swgfl.org.uk/>\)](#) It includes presenter notes to make it easy to confidently cascade to all staff



Training – Governors

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

- Attendance at training provided by the National Governors Association or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure, equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by WGGs. Users are responsible for the security of their username and password and will be required to change their password every term.
- The administrator passwords for the school ICT system, used by the System support contractors must also be available to the IT Lead or other nominated senior leader and kept in a secure place online. Passwords will not be recorded on paper.
- The school's technical staff are responsible for ensuring that software licence are accurate and up to date and that regular checks are made to ensure the number of licences are both adequate and necessary. (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch



Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored by WGGs. There is a clear process in place to deal with requests for filtering changes by logging calls with WGGs

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – teaching staff / pupils / office staff etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate system are in place (**Whisper / Every**) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure is protected by its cloud based suppliers and broadband provider.
- An agreed policy is in place (**to be described**) for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems. **In our first years this will be by use of the ‘Test Teacher / Test TA’users.**
- **Since the School only uses Chromebooks which are cloud based devices any user can safely use them provided they use their own personal login credentials. School logins are never to be shared or circumvented.**
- An agreed policy is in place (**to be described**) that allows staff to / forbids staff **from downloading executable files onto the school’s remote desktop infrastructure. Chrome Applications and Extensions and LearnPad lessons and applications may be freely searched for and added to their profiles provided that:**
 - they are appropriate for use in school;
 - they are notified to the Online Safety Group using Every
 - no paid application is downloaded without the Head Teacher’s prior written permission;
 - In future it is intended that the school will populate a St John’s Online Store of approved Applications and Extensions but in the first years of the school the appropriate suite of applications will be established by practical use and recommendation from the school’s IT provider, Joskos.
- An agreed policy is in place prohibiting the use of removable media (eg memory sticks / CDs / DVDs) by users on all school devices. **Personal data may never leave the school on any of these media.**



- **Where data arrives at the school on these types of devices they must be given to the WGS for transfer onto the school's cloud based system or, if urgent and appropriate, to the school Office.**

Personal data may not be sent by email or transferred over the internet or taken off the school site. Where necessary data is shared via Google Drive the clear Folder naming convention of 'Sharedwith..' must be used so that users are clear when data is shared.

Sharing permissions are only set at folder level (meaning that individual documents are not especially shared with individual people. Internally folders are only restricted as necessary and only by use of pre-set groups: teaching staff, HR people, Finance people etc NOT individuals.

Mobile Technologies (including BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, Chromebook, laptop or other technology that usually has the capability of utilising the schools wireless network. The device then has access to the internet and, **subject to user rights and passwords, to the school's other cloud based services. By Policy and User Agreement school systems will always be accessed via RM Unify – the school's landing page – and not accessed directly. This will apply whether using a school device or a user's own device and whether accessing using the school's wireless network or at any other location.**

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behavior Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- **The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies**
- **The school allows:** (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			Personal Devices		
	School owned for single user	School owned for	Authorised device ¹	Student owned	Staff owned	Visitor owned

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.



		multiple users				
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Internet only	Yes	Yes	Yes	No	Yes	Yes



Aspects that the school may wish to consider and be included in their Online Safety Policy, Mobile Technologies Policy or Acceptable Use Agreements:

The following items will be discussed and specifically defined by the Online Safety Group completing the first comprehensive statement within the school's first year:

School owned / provided devices:

- Who they will be allocated to
- Where, when and how their use is allowed – times / places / in school / out of school
- If personal use is allowed
- Levels of access to networks / internet (as above)
- Management of devices / installation of apps / changing of settings / monitoring
- Network / broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking / storage / use of images
- Exit processes – what happens to devices / software / apps / stored data if user leaves the school
- Liability for damage
- Staff training

Personal devices:

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



- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press by use of the AUA signed by parents or carers - see Parents / Carers Acceptable Use Agreement in the appendix)
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.



- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents



- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- **Transfer data only using Google sharing. The Head Teacher and Office staff may also, when required, transfer Personal data using the government gateway, via Scholarpack and Hertfordshire's Local Authority systems eg for admissions.**
- **Removable storage devices will never be used for exchanging Personal data outside the school even if encrypted and passworded. Data arriving on such devices MUST be uploaded by the school office staff who will take technical advice if necessary.**
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

This is an area of rapidly developing technologies and uses. Schools / academies will need to discuss and agree how they intend to implement and use these technologies eg some schools do not allow pupils to use mobile phones in lessons, while others recognise their educational potential and allow their use. This section may also be influenced by the age of the students / pupils. The table has been left blank for school to choose its own responses.

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:

The following items will be discussed and specifically defined by the Online Safety Group completing the first comprehensive statement within the school's first year: Until that time all are prohibited.



	Staff & other adults			Students / Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
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 other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school , or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others about school matters. Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. They may do so anonymously using **Whisper**.



- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, personal text messaging or personal social media must not be used for these communications.
- Pupils will be provided with individual school email addresses for educational use. In EYFS and KS1 common class-wide passwords will be used.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school group 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:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. [Online Safety BOOST includes unlimited webinar training on this subject: https://boost.swgfl.org.uk/](https://boost.swgfl.org.uk/)
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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



The school's official social media accounts are established and there is:

- A process for approval by senior leaders

The following items will be discussed and specifically defined by the Online Safety Group completing the first comprehensive statement within the school's first year:

- *Clear processes for the administration and monitoring of these accounts*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, 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 for personal use **on personal devices and possibly on school devices if requested.**

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies. Online Safety BOOST includes Reputation Alerts that highlight any reference to the school/academy in online media (newspaper or social media for example) <https://boost.swgfl.org.uk/>

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities



e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated 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 (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing via Google Drive		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

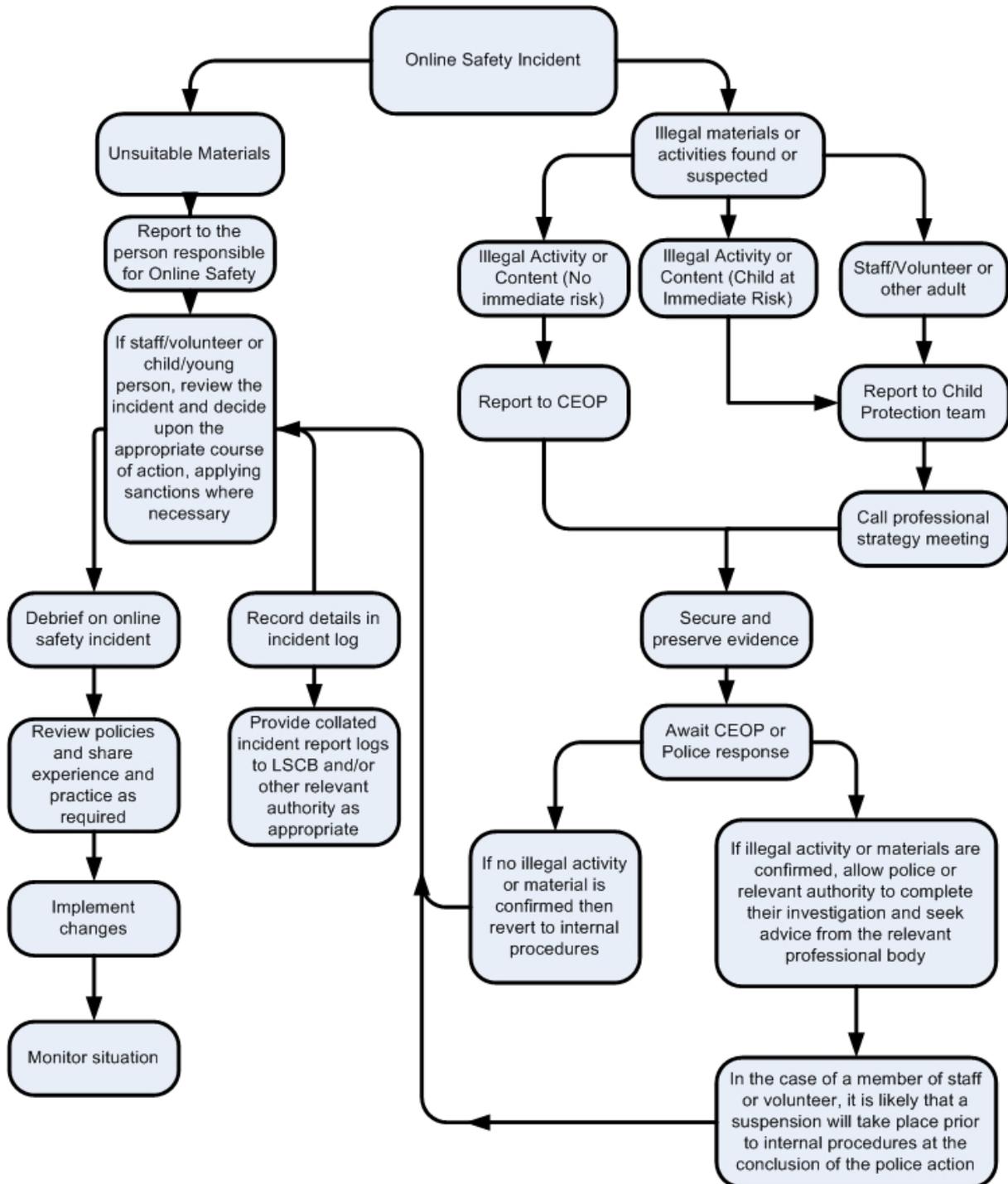
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above). [Online Safety BOOST includes a comprehensive and interactive ‘Incident Management Tool’ that steps staff through how to respond, forms to complete and action to take when managing reported incidents \(<https://boost.swgfl.org.uk/>\)](#)



Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) 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:
 - Internal response or discipline procedures
 - Involvement by 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 **and immediately ask WGGs to disable the individuals log on providing access to their school RM Unify and Google accounts.** 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:

The following items will be discussed and specifically defined by the Online Safety Group completing the first comprehensive statement within the school's first year:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons									
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device									
Unauthorised / inappropriate use of social media / messaging apps / personal email									



Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another student's / pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school 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									

Actions / Sanctions

Staff Incidents

	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support 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				



Inappropriate personal use of the internet / social media / personal email	X					
Unauthorised downloading or uploading of files	X					
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X	
Deliberate actions to breach data protection or network security rules	X				X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X				X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X					
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X					
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						



Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

<http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy>

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (esafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2016.