St Paul's C.E Primary School

Building each other up –
with God as our firm foundation

Online Safety Policy

Policy Created/reviewed: September 2023

Approved by Governing Body: September 23

Policy published: September 2023

Policy Review: September 2024

2023 updates;

Roles and responsibilities updated to reflect new Online Safety Leader and IT Technician / provider.

SENSO monitoring added

Contents

Development/Monitoring/Review of this Policy

This online safety policy has been developed in collaboration with:

- Headteacher and senior leaders
- Online Safety Leader
- Staff – including teachers, support staff, technical staff
- Governors/Board

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	*April 23*
The implementation of this online safety policy will be monitored by:	*J Ferretti (Headteacher/Online Safety Leader)* *L Davis (Deputy Headteacher)* *R Cook (Computing Leader)*
Monitoring will take place at regular intervals:	*Twice yearly*
The Board of Directors/Governing Body/Governors Sub Committee will receive a report on the implementation of the online safety policy generated by the Online Safety Leader	*Once a year*
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:	*September 2023*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Safeguarding Advisor, Governing Body, MASH, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/pupils
    - parents/carers
    - staff

Scope of the Policy

This policy applies to all members of the *St Paul's* community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school/academy digital technology systems, both in and out of the *school.*

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the *school*, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of

electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

St Paul's CofE Primary School will deal with such incidents within this policy and associated Behaviour and Anti-bullying Policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Full Governing Body or Safeguarding Committee who will* receive regular information about online safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Safety Governor*: Leanne Clarke.

The role of the Online Safety *Governor* will include:

- regular meetings with the Online Safety Leader
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting

Headteacher and Senior Leaders

- The *Headteacher* 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 Lead*.
- The Headteacher 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 *Local Authority/MAT/other relevant body* 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. More information is available at: https://boost.swgfl.org.uk/
- *The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.* Online Safety BOOST includes access to unlimited online webinar training – further details are at https://boost.swgfl.org.uk/

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. At St Paul's we use Lightspeed as our Filtering System, which is provided by the council but controlled by the school's technician and Online Safety Leader. We use SENSO to monitor the use of devices by adults and pupils.

- *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

Online Safety Lead – Mrs J. Ferretti

- 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 the Local Authority/relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (Examples of suitable log sheets may be found later in this document). 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 https://boost.swgfl.org.uk/
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of *Governors*
- reports regularly to Senior Leadership Team

Network Manager/Technical staff – Miss C. James

Those with technical responsibilities 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 *Local Authority/other relevant body* online safety policy/guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy**
- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person* (see appendix "Technical Security Policy Template" for good practice)
- 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 *networks/internet/digital technologies* is regularly monitored in order that any misuse/attempted misuse can be reported to the *Headteacher and Senior Leaders; Online Safety Lead* for investigation/action/sanction
- *that monitoring software/systems are implemented and updated as agreed in school/academy policies*

Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current *school* Online Safety Policy and practices**
- **they have read, understood and signed the staff Acceptable Use Policy/Agreement (AUP/AUA)**
- **they report any suspected misuse or problem to the *Headteacher/Senior Leader/Online Safety Lead* for investigation/action/sanction**
- **all digital communications with students/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
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/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 students/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/Designated Person/Officer

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

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Group

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

Members of the Online Safety Group will assist the Online Safety Lead with:

- the annual review of the school online safety policy/documents and review in response to an incident.
- *monitoring the online safety incident log.*
- *monitoring of the school filtering systems*
- *discussing training needs including staff, parents, pupils and community.*
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool
- plan online safety events

Membership:
The Online Safety Group will include the school's;

Online Safety Leader
Headteacher or Deputy Headteacher (D/DSL)
Computing Leader
IT Technician
Parent representatives
Pupil representatives
Governor representative
External advisor (as required)

Pupils:

- **are responsible for using the *school's* digital technology systems in accordance with the pupil Acceptable Use Policy / 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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's/academy'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, social media 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/Learning Platform and on-line student/pupil records
- *their children's personal devices in the school (where this is allowed)*

Community Users

Community Users who access school systems or programmes as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school/academy systems. (A community users acceptable use agreement template can be found in the appendices.)

Policy Statements

Education – Pupils

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

In planning their online safety curriculum schools/academies may wish to refer to:

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- SWGfL Project Evolve – online safety curriculum programme and resources

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 worship and 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**

- **Students/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.** N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- *Students/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 students/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 students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical 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 online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- *Curriculum activities*
- *Letters, newsletters, web site, Google Classroom, Twitter*
- *Parents/carers evenings/sessions*
- *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 *(see appendix for further links/resources)*

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/academy website will provide online safety information for the wider community*

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 (https://boost.swgfl.org.uk/)
- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.** Online Safety BOOST includes an array of presentations and resources that can be presented to new staff (https://boost.swgfl.org.uk/)
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.*
- *The Online Safety Lead (or other nominated 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 group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

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

Technical – infrastructure/equipment, filtering and monitoring

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

A password is required in order to access the school and have flexibilty.

The school's technician is able to login to Lightspeed and monitor, using a member of staffs or pupil's login details and view their website history for the last 90 days. This is monitored and reviewed by the Online Safety Team.

- **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** J Ferretti (IT Leader) or C James (Technician) *who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password**.
- The "master/administrator" passwords for the school/academy systems, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (e.g. school safe)
- C James is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Requests should be discussed with the Headteacher. If authorised, the school's technician logs onto Lightspeed and is able to block or unblock websites.
- **Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet**
- *The school has provided enhanced/differentiated user-level filtering enabling staff to access certain websites children cannot.*
- *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 Policy / Agreement.*
- *An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed). An incident sheet is used for pupils to complete with a member of staff. Staff report issues via a helpdesk tab on the school platform.*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software (Windows Defender).
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- *Users (staff/students/pupils/community users) and their family members should not use school devices for personal activity.*
- *A system is in place that prevents staff from downloading certain executable files and installing programmes on school devices.*
- *An agreed policy is in place allowing the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices.* ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured***.

- All staff laptops are secured by Bitlocker and require a password to access them. All portable hard drives used in school should be Bitlocker protected and require a password to access.
- All social media websites are blocked by default by the council and can only be unblocked by the school's technician.

Mobile Technologies (including BYOD/BYOT (Bring Your Own Device/Technology))

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

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-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:**

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*			
Internet Only					*Yes*	*Yes*
No network access						

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

School owned/provided devices:

- *Who they will be allocated to – Teachers, Teaching Assistants, Admin Assistants, School Business Manager, SLT.*
- *Where, when and how their use is allowed – determined by staff members*
- *If personal use is allowed- no*
- *Levels of access to networks/internet – depends on access level of the user*
- *Management of devices/installation of apps/changing of settings/monitoring*
- *Network/broadband capacity We currently have a 100mb broadband, which will be increased to 1gb via the council in the future.*
- *Technical support – Charlotte James – IT Technician – e-services*
- *Filtering of devices- Lightspeed*
- *Access to cloud services - All staff have access to Cloud Service via CloudW from Wolverhampton eservices through school platform.*
- *Data Protection*
- *Taking/storage/use of images images can only be taken on school devices, which are password protected.*
- *Exit processes – what happens to devices/software/apps/stored data if user leaves the school - staff are removed from school server & school platform access is removed. Staff laptops are collected, formatted and rebuilt.*
- *Staff training Delivered in house or carried out by external provider e.g. Squirrel Learning.*

[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.

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 (office areas, staffrooms, empty classrooms.)
- Storage (cupboard, bag locked away.)
- Whether staff will be allowed to use personal devices for school business – no school files should be downloaded or saved to personal devices. Staff are able to access and send emails on personal phones.
- Levels of access to networks/internet (as above)
- Staff can access the school network/internet for personal devices.
- 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 (school devices only)
- 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 students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

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

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **Specific, written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *pupils* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- 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 current data protection legislation.

The school/academy must ensure that:

- **it has a Data Protection Policy.**
- **it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.**
- **it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).**
- **it has appointed an appropriate Data Protection Officer (DPO) (LA) who has a high level of understanding of data protection law and is free from any conflict of interest.**
- **it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it**
- **the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded**
- **it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Systems should be in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals**
- **it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice** (see Privacy Notice section in the appendix)
- **procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).**
- **Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)**
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

- **it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.**
- **it understands how to share data lawfully and safely with other relevant data controllers.**
- **it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.**
- **if a maintained school it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.**

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

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

Staff must ensure that they:

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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults			*Students/Pupils*				
Communication Technologies	Allowed	Allowed at certain times/in certain areas	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school/academy	*				*			
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/academy, or on school/academy network				*				*
Use of school/academy email for personal emails				*				*
Use of messaging apps (only on personal devices)		*						*
Use of social media (only on personal devices, unless authorised school social media)		*						*
Use of blogs (only on personal devices, unless authorised school blog)		*						*

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 when in school, or on school systems (e.g. by remote access).*
- **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.** (Online Safety BOOST includes an anonymous reporting app Whisper – https://boost.swgfl.org.uk/)

- **Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *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/academy website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school/academy protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools/academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school/academy 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/
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School/academy staff should ensure that:

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

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

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including;*
    - *Systems for reporting and dealing with abuse and misuse*
    - *Understanding of how incidents may be dealt with under school/academy disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school/academy permits reasonable and appropriate access to private social media sites*

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/)

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school/academy 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/academy context and that users, as defined below, should not engage in these activities in/or outside the school/academy when using school/academy equipment or systems. The school/academy 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 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X

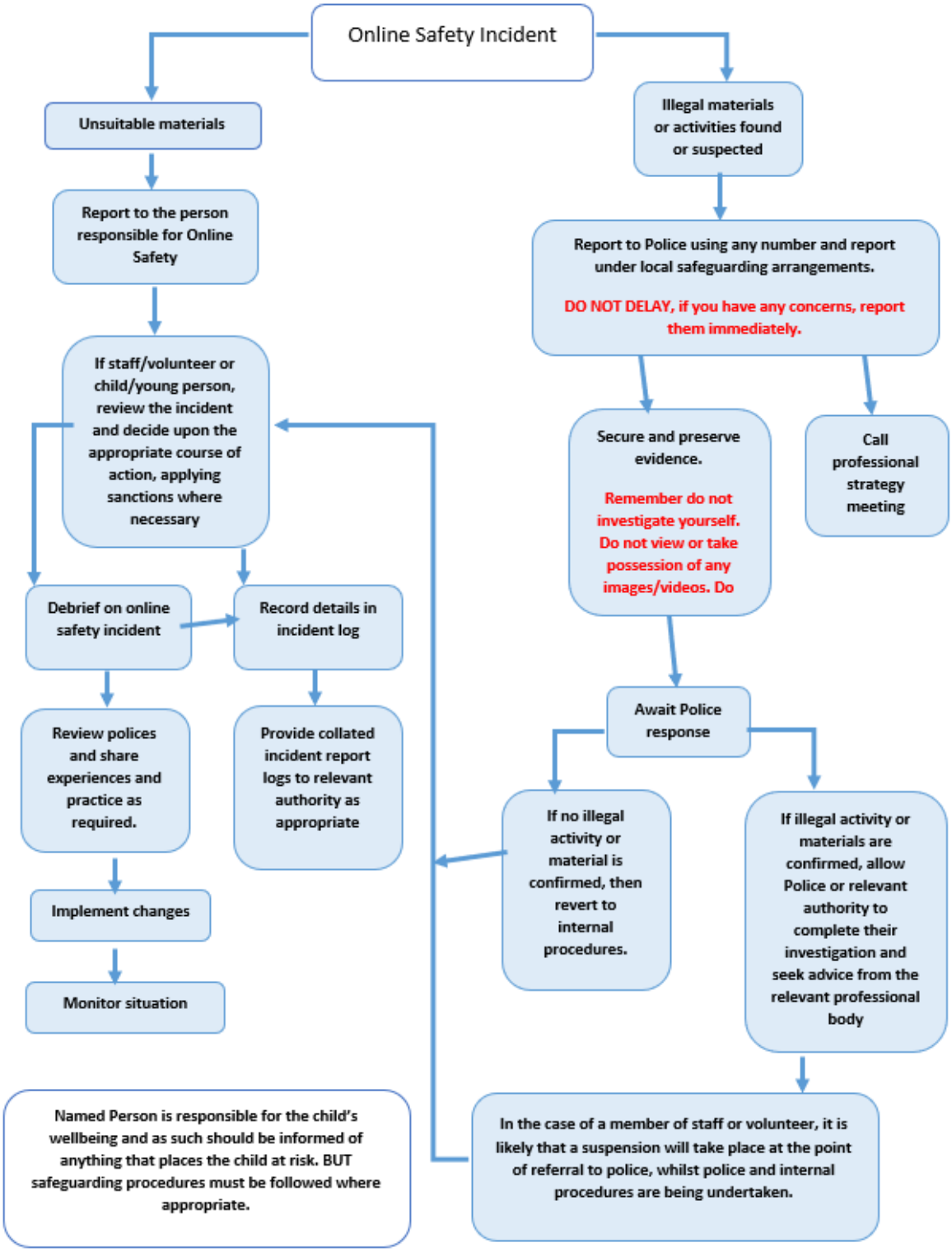
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)	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


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

Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

	Actions/Sanctions								
Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Head of Department/Year/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 e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X		X	X		X
Unauthorised use of non-educational sites during lessons	X	X	X			X		X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		X	X	(X)		X		X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email		X	X	(X)		X	X	X	X
Unauthorised downloading or uploading of files		X	X	(X)		X	X	X	X
Allowing others to access school/academy network by sharing username and passwords			X		X	X	X		X
Attempting to access or accessing the school/academy network, using another student's/pupil's account		X	X		X	X		X	X
Attempting to access or accessing the school/academy network, using the account of a member of staff		X	X		X	X		X	X
Corrupting or destroying the data of other users		X	X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	(X)	X	X		X

Continued infringements of the above, following previous warnings or sanctions			X	(X)		X			X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X		X	X
Using proxy sites or other means to subvert the school's/academy's filtering system		X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X	X	X	X	X		X
Deliberately accessing or trying to access offensive or pornographic material			X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X	X		X

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	X				
Inappropriate personal use of the internet/social media/personal email		X				X	X	X
Unauthorised downloading or uploading of files		X			X	X	X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X	X	
Deliberate actions to breach data protection or network security rules		X			X		X	X

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X		X	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X	X			X	X	X
Actions which could compromise the staff member's professional standing		X				X	X	X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy		X				X	X	X
Using proxy sites or other means to subvert the school's/academy's filtering system		X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Breaching copyright or licensing regulations		X				X	X	X
Continued infringements of the above, following previous warnings or sanctions		X						

Appendix

Copies of the more detailed template policies and agreements can be downloaded from:

SWGfL Online Safety Policy Templates

Acknowledgements

SWGfL would like to acknowledge the contribution of a wide range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the online safety policy templates and of the 360 degree safe online safety self-review tool.

This policy should be read in conjunction with

- Safeguarding and Child Protection Policy
- Anti -Bullying Policy
- Staff Code of Conduct Policy
- Social Media Policy