Online Safety Policy

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Willand School to safeguard members of our school community online in accordance with statutory guidance and best practice.
This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).
Willand 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.

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development, Monitoring and Review of this Policy

This online safety policy has been developed by a working group made up of:

- School Online Safety Lead (Pauline Maynard)
- Headteacher (Anne Hawkins) and Senior Management Team
- Designated Safeguarding Lead (Amy Leather)
- SENDCo (Hannah Telling)
- Teachers
- Support Staff
- Governors
- Parents and Carers

Schedule for the Development, Monitoring and Review of this Policy

The online safety policy was approved by the Governing Body on:	27/11/23
The implementation of this online safety policy will be monitored by:	Online Safety Lead (Pauline Maynard) Senior Management Team and Governors
Monitoring will take place at regular intervals:	At least annually.
The Governing Body will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals.	Termly, within the Online Safety Lead's feedback to the Headteacher. This will then be included in the Headteacher report to Governors.
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:	November 24 and annually thereafter
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Police LA ICT Manager LA Safeguarding Officer

The school will monitor the impact of the policy using:

- Logs of reported incidents (with the aid of CPOMs)
- ScoMIS monitoring of computer use throughout the school
- Annual survey of pupils and parents (linked with Safer Internet Day)
- Pupil representative feedback to the computing co-ordinator
- SWGfL monitoring logs of internet activity
- Internal monitoring data for network activity

Roles and Responsibilities

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. 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/Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- checking that provision outlined in the Online Safety Policy (e.g. education provision and staff training) is taking place as intended.
- reporting to relevant Governors/Board/Committee/meeting
- Receiving (at least) basic cyber security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.

Headteacher and Senior Leaders

- The **Headteacher** has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The **Headteacher and Senior Leaders** are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues.
- 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 the important monitoring role. The Online Safety Lead will monitor online safety incidents on CPOMs, the filtering log and SWGfL log of internet misuse.
- The **Senior Leaders** will receive regular monitoring reports from the Online Safety Lead.
- The **Headteacher and Senior Leaders** are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see SWGfL flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures)
- The **Headteacher and Senior Leaders** will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Online Safety Lead

The Online Safety Lead takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy. They:

- work in support of and report to the Designated Safeguarding Lead (DSL) who holds the overall responsibility for online safety.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide (or identify sources of) training and advice for staff
- liaise with the Local Authority
- liaise with school ICT technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meet regularly with the relevant Governor to discuss current issues
- report regularly to Senior Leadership Team

<u>All incidents will be recorded on CPOMS;</u>
<u>Designated Safeguarding Lead, Headteacher and Online Safety Lead will be alerted.</u>

Network Manager

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access school systems through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he / she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Designated Safeguarding Lead, Online Safety Lead and Headteacher for investigation
- that monitoring software and systems are implemented and updated as agreed in school policies.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Teaching and Support Staff

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 understand that online safety is a core part of safeguarding
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Designated Safeguarding Lead, Online Safety Lead and Headteacher for investigation / action / sanction

- digital communications with pupils 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 school activities
- pupils understand and follow the school online safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Designated Safeguarding Lead

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection 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

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- **be responsible for receiving reports of online safety incidents and handling them,** and deciding whether to make a referral by liaising with relevant agencies, **ensuring that all incidents are recorded**.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

The DSL may delegate any of the above duties to the Online Safety Lead but will continue to hold responsibility.

Pupils

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (NB: KS2 pupils will sign it once a year in school with their parents being given the information about what the children have signed. KS1 pupils (not Reception) will sign every year with their parents being given the information about what the children have signed and a link to an optional google form to sign). This will be undertaken during the first month of each new school year.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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 and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues, e.g. through parents' workshops, raising awareness through the school website and newsletters, whole-school assemblies where classes tackle different aspects of online, making parents aware of sources of information online.

Parents and carers will be responsible for:

- reading and supporting their child in adhering to the school's Acceptable Use Policy.
- accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy**.**
- supporting the school in reinforcing the online safety messages provided to learners in school.

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 education will be provided in the following ways:

- A planned online safety programme of progression will be provided as part of the computing and PSHE curriculum. Elements of the programme will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school;
- Key online safety messages will be reinforced as part of a planned programme of assemblies;
- Opportunities for exploring online safety in other curriculum areas will be encouraged. For example, within History and English, pupils will be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Rules for use of ICT systems / internet will be posted in all classrooms;
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

- Letters
- Leaflets
- Parent workshops
- Regularly updated links to online safety resources via the website and newsletter updates
- Incorporating online safety awareness into class assemblies

Education - Extended Schools

The school will offer/signpost family workshops, media literacy and online safety so that parents and children can together gain a better understanding of these issues. Messages to the public around online safety will also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy technology, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

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. An audit of the online safety training needs of all staff will be carried out regularly;

- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies;
- The Online Safety Lead will receive regular updates through attendance at SWGfL / LA /other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others;
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days;
- The Online Safety Leads will provide advice / guidance / training as required to individuals.

Training – Governors

Governors should take part in our regular cycle of online safety training / awareness sessions, with particular importance for those who are responsible for Health and Safety and Safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association /SWGfL or other relevant organisation;
- Participation in school training and information sessions for staff or parents.

A higher level of training will be made available, if possible, to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Technical – infrastructure / equipment, filtering and monitoring

The school ensures that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school ensures that all staff are made aware of policies and procedures on a regular basis and explains that everyone is responsible for online safety and data protection.

The school filtering and monitoring provision is agreed by senior leaders, DSL, governors and SCOMiS and is regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours. The DSL has lead responsibility for safeguarding and online safety and SCOMiS has technical responsibility.

SCOMiS and RM Safetynet have the technical responsibility for maintaining the filtering and monitoring system and providing reports. Reviewing and acting on these reports will the responsibility of the DSL supported by the OSL. SWGfL test filtering tool will be used regularly on pupil and staff devices to check the efficacy of the filtering in place.

Filtering

- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated

- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- requests/approvals for filtering changes should be directed to the DSL
- filtering logs are regularly reviewed and acted upon where necessary.
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users: staff/learners
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- pupils are supervised at all times when using devices that can access the internet;
- pupils are monitored by staff whilst they are using the internet. They report any concerns to the Online Safety Lead. Where there is concern for safeguarding, this is also reported to the DSL;
- the filter is monitored by the DSL and Online Safety Lead each term on a range of devices across the school using https://testfiltering.com/;
- the DSL regularly checks the RMSafetyNet Reporting Tool for the top ten searches and recent searches;
- the DSL and Online Safety Lead regularly check pupil work folders for a range of inappropriate terms;
- when inappropriate sites that are unblocked are found, the filter will be updated to prevent further access;
- all users are aware that the network (and devices) are monitored;
- monitoring strategy is led by the DSL.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements .

- responsibility for technical security resides with SMT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by SCOMiS and will be reviewed, regularly, by SMT.
- password policy and procedures are implemented.
- the security of staff usernames and password and must not allow other users to access the systems using their log on details.
- all staff have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- school networks and systems will be protected by passwords. Staff passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems

- appropriate security measures are in place to protect the ~~servers~~, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data.
- there are rigorous and verified back-up routines
- The school business manager is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail)
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile.

Curriculum

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of computing across the curriculum.
- 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, e.g. using search engines, 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant 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.
- 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.

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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;
- Permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press;
- 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 or volunteers should not be used for such purposes unless permission is given by the Headteacher;
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school/academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital/video images;
- 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 will 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) who has a high level of understanding of data protection law and is free from any conflict of interest. The school/academy may also wish to appoint a Data Manager and Systems Controllers to support the DPO;
- 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. Have systems 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/academy 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;
- It has 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 (be sure to select devices that can be protected in this way);
- 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 policy once it has been transferred or its use is complete.

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;
- 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 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

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, 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 learning platform and other cloud-based services such as e-mail and data storage.

Risks associated with the use of such mobile technologies may include:

- security risks in allowing connections to the school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices		**Personal devices**		
	School owned for individual use	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	Yes	Yes	Yes
Network access	Yes	Yes	No	No	No

School owned/provided devices:

- *some school devices are managed though the use of Jamf software*
- *there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed*
- *any designated mobile-free zone is clearly signposted*
- *personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.*
- *the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.*
- *liability for damage aligns with current school policy for the replacement of equipment.*
- *education is in place to support responsible use.*

Personal devices:

- *there is a clear policy covering the use of personal mobile devices on school premises for all users*
- *where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.*
- *where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.*

- *use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems*
- *the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.*
- *liability for loss/damage or malfunction of personal devices is clearly defined*
- *there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements*
- *education about the safe and responsible use of mobile devices is included in the school online safety education programmes*

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 and other adults				Pupils			
Communication Technologies	**Allowed**	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed for selected pupils**	**Not allowed**
Personal mobile phones may be brought to the school/academy	✓				✓			
Use of personal mobile phones in lessons				✓				✓
Use of personal mobile phones during educational visits	✓							✓
Use of personal mobile phones in social time	✓							✓
Taking photos on personal mobile phones/cameras			✓					✓
Use of other personal 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		✓						**N/a**
Use of messaging apps on school devices				✓				✓
Use of messaging apps on personal devices		✓						✓
Use of social media on school devices			✓					✓
Use of social media on personal devices		✓						✓
Use of blogs on school devices			✓					✓
Use of blogs on personal devices		✓						✓

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 need to be aware that email communications may be monitored;
- Users must immediately report, to the Headteacher – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email;
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications. The only exception is communication on a personal level of any longstanding friendships between staff and parents prior to this policy being implemented;
- Whole class or group email addresses will be used at KS1 and KS2 for educational use;

- Pupils must be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material;
- 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

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

Willand 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;
- Information is made available to staff including: acceptable use; social media risks; checking of settings; data protection; reporting issues;
- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.

Staff should ensure that:

- No reference should be made in social media to students/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;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

School Social Media Account

Willand School has a social media account to share information with parents and carers. The Headteacher is responsible for ensuring that the member/s of staff running this account on behalf of the school has/have read and understood this policy and received appropriate training.

The school account is monitored regularly and frequently. It has restrictions on each post to prevent any comments being posted.

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.
- The school permits reasonable and appropriate access to private social media sites
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Further information can be found in the DCC Policy For Employees And Adults Associated With Schools Using And Participating In Social Media.

Unsuitable / inappropriate activities

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

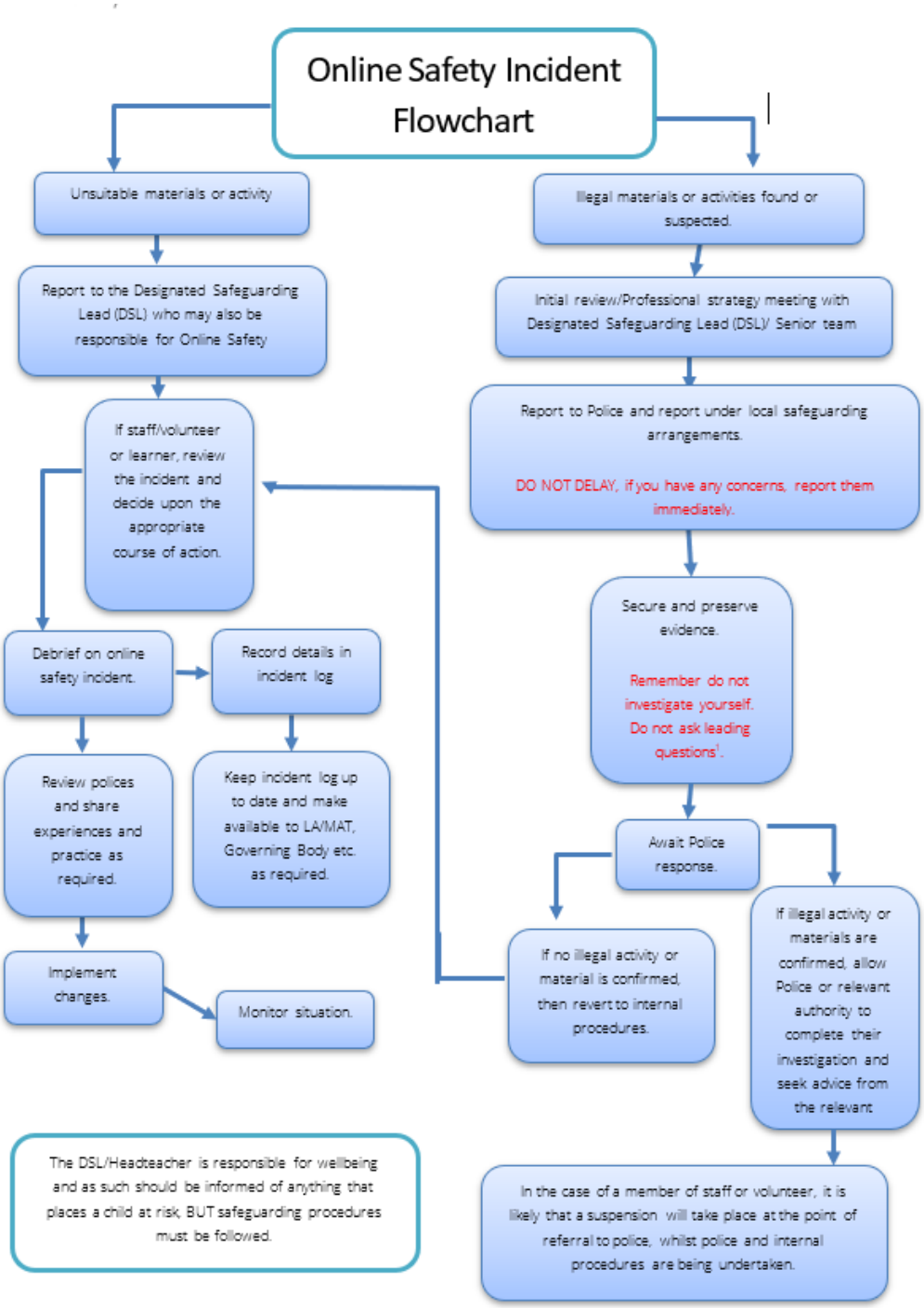
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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, gambling or drugs				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: • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • 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)						X

• Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
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				
Use of social media			X		
Use of messaging apps	X				
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported;
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure;
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection);
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below);
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority Designated Officer (LADO)
    - 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.

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								
Pupils Incidents	Refer to class teacher	Refer to Key Stage Co-ordinator	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of 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).	✓		✓	✓	✓	✓			✓
Unauthorised use of non-educational sites during lessons	✓		✓				✓		
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	✓		✓					✓	
Unauthorised/inappropriate use of social media/ messaging apps/personal email	✓		✓				✓	✓	
Unauthorised downloading or uploading of files	✓		✓		✓		✓	✓	
Allowing others to access school/academy network by sharing username and passwords	✓		✓		✓	✓	✓	✓	
Attempting to access or accessing the school/academy network, using another student's/pupil's account	✓		✓				✓	✓	
Attempting to access or accessing the school/academy network, using the account of a member of staff	✓		✓			✓	✓	✓	✓
Corrupting or destroying the data of other users	✓		✓			✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓		✓		✓	✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓		✓	✓	✓	✓	✓
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school	✓		✓		✓	✓	✓	✓	✓
Using proxy sites or other means to subvert the school's/academy's filtering system	✓		✓		✓	✓	✓	✓	✓

Accidentally accessing offensive or pornographic material and failing to report the incident	✓		✓		✓	✓	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓		✓		✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓		✓			✓	

POLICY HISTORY

Policy Date	Summary of change	Contact	Version/ Implementation Date	Review Date
16/7/14	New policy	IM	21/7/14	Jul 17
27/03/17	Updated	PM	27/04/17	May 20
19/06/20	Updated	PM	02/07/2020	Jun 21
22/04/21	No Changes	PM	29/04/2021	Apr 22
05/05/22	Slight changes of terminology Review of communication technology best practice Addition of mobile technology section Addition of social media section Update to incident flow chart Review of staff and pupil actions / sanctions Review of acceptable use agreements	PM / AL	17/11/22	Nov 23
13/11/23	Sections amended to reflect new guidance on filtering and monitoring: Scope Technical security Sections amended to reflect new guidance on the enhanced online safety role of the DSL and governors: Responsibilities of governors, head teacher, DSL, OSL, network manager Mobile technologies section re-written to reflect advice from SWGFL. Parents and carers section amended. Additional training requirement for online safety governor. Complete rewrite of technical security, filtering and monitoring section in line KCSiE 2023 and SWGFL advice.	PM	13/11/23	Nov 24