WISHFORD SCHOOLS

ONLINE SAFETY POLICY

This Policies applies to all Wishford Schools including all EYFS settings.

Date of Policy	**September 2023**
Member of staff responsible	**Mr Andrew Webster**
Role	**Head of Compliance (inc Online Safety Director)**
Review date	

Last Review	**Significant changes**

1. Policy Scope

This policy applies to pupils and all parents, visitors and staff across Wishford schools[1]; including the governing body, leadership teams, teachers, support staff, external contractors, volunteers and other individuals who work for, or provide services on behalf of our settings, e.g. guest speakers (collectively referred to as **"users"** in this policy).

This policy should be read in conjunction with the group's **IT Acceptable Use Policy and Privacy Notice & Data Protection Policy**. Other related school level policies include:

- Safeguarding policy
- Anti-Bullying policy
- Behaviour policy
- The staff handbook
- Curriculum policies, such as: Personal Social Health and Economic Education (PSHEE) and Relationships and Sex Education (RSE)

This policy was written with regard to:

- Keeping Children Safe in Education, 2023;
- Early Years and Foundation Stage, 2021;
- Working Together to Safeguard Children, 2018;
- Behaviour in Schools: Advice for headteachers and school staff, 2022;
- Searching, screening and confiscation at school, 2022; and
- Teaching online safety in schools, 2019.

Aims: This policy aims to:

Safeguard and promote the welfare of all members of the Wishford community in relation to any online activity, both in and out of school.

Implementation: There are two main features of the implementation of this policy:

1. **Prevention**: robust and responsive systems for filtering and monitoring online activity.
2. **Education**: training users to be responsible, discerning and considerate whilst online.

Staying safe online requires a multi-layered approach which includes filtering, monitoring, education, clear consequences and pastoral support. It would not be in the educational interest of our pupils to block the internet entirely and so we rely on all users to engage with regular and effective communication regarding online safety so we can use the internet to achieve the best possible educational outcomes whilst also keeping everyone safe.

All users are updated at least **annually** on the guidance outlined in this policy. It forms part of the induction process for all new staff, parents and pupils. Pupils will be educated regarding safe and appropriate online activity and will be made aware of behaviour expectations and consequences for policy breaches.

This policy is updated every two years or following any local or national updates or changes in our technical infrastructure. Internal monitoring and risk assessment may also lead to policy updates. This policy may also be reviewed following an online safety incident.

[1] The term 'schools' applies here to all organisations within the Wishford group including nurseries and camps.

2. Roles & Responsibilities

Proprietor

The Proprietor is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This responsibility is delegated to the **Online Safety Director** whose responsibilities include:

- Updating the Proprietor and Group Operations team on all developments.
- Chairing regular meetings with School Online Safety Co-ordinators and the Group Head of Technology.
- Termly monitoring of online safety incident logs and monitoring/filtering logs in each school.
- Reviewing and updating the central policy template, ensuring it is in line with the most up-to-date guidance and regulations.
- Recommending training and advice for Online Safety Leads.
- Liaising with Group IT to resolve technical risks affecting all schools.
- Reviewing online safety incident trends and logs to inform future online safety developments.

Group Head of Technology and Technical Staff

Are responsible for ensuring:

- That the Group's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the Group meets required online safety technical requirements and any 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 system.
- That filtering/monitoring systems are applied and updated on a regular basis and in line with current regulations; and that their implementation is not the sole responsibility of any single person.
- 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/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to Headteachers, the Group Online Safety Director, Senior Leaders and Online Safety Leads for investigation/action/sanction.

Headteachers 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 school's Online Safety Lead.
- The Headteacher and (at least) one other 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 (appendix 3) on dealing with online safety incidents. The Head should also be aware of local authority guidance/procedures.
- 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.
- 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.
- The Senior Leadership Team in each school will receive regular monitoring reports from the school's Online Safety Co-ordinator.

Online Safety Lead

Each school must have a named member of staff with a day to day responsibility for online safety, some schools may choose to combine this with the Designated Safeguarding Lead role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school. The Online Safety Lead:

- Oversees the Online Safety Development Plan.
- Leads the school's Online Safety Committee and participates in termly, group-wide meetings.
- Takes day to day responsibility for online safety issues and establishes and reviews school online safety policies/documents.
- Ensures that all school staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Arranges or provides training and advice for school staff.
- Liaises with the Local Authority.
- Escalates technical issues for resolution to the Group IT Team.
- 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).
- Meets regularly with the Head and Online Safety Director to discuss current issues, review incident Logs and maintains filtering/change control logs.
- Attends relevant meetings at both group and school level.
- Reports regularly to Senior Leadership Team.

(N.B. The school will need to decide how online safety incidents will be dealt with and whether the investigation/action/sanctions will be the responsibility of the Online Safety Lead or another member of staff e.g. Headteacher/Senior Leader/Designated Safeguarding Lead/Class teacher/Head of Year etc.)

Designated Safeguarding Lead

- 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.
- (N.B. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop. Some schools may choose to combine the roles of Designated Safeguarding Lead and Online Safety Lead).

Online Safety Group

The Online Safety Group operates at two levels: group wide (the Online Safety Committee with a single representative from each school) and at school level (school Online Safety Groups, chaired by the Online Safety Lead). Both levels provide a consultative group that has wide representation, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of new threats and initiatives. Depending on the size or structure of the school some groups may be part of the safeguarding group. School Online Safety Groups will also be responsible for regular reporting to the Group Online Safety Committee, who in turn will report to the Proprietor.

Members of the Online Safety Committee or Groups will assist the Online Safety Director and School Leads with:

- The production/review/monitoring of online safety policy/documents.
- The production/review/monitoring of filtering policy and requests for filtering changes.
- Mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression.
- Monitoring network/internet/filtering/incident logs.
- 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.
- (N.B. Schools will need to decide the membership of the Online Safety Group. It is recommended that the group should include representation from students/pupils).

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 IT Acceptable Use Agreement and that they follow the guidance contained therein.
- They report any suspected misuse or problem to the Online Safety Lead, escalating concerns to the Headteacher or Director of Online Safety as necessary.
- All digital communications with students/pupils/parents/carers are professional 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 physically 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 any unsuitable material that is found in internet searches is reported for blacklisting.

Students/Pupils:

- Are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement.
- 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 Group'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. Schools should 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 should 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.
- 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 an IT Acceptable Use Agreement before being provided with access to school systems.

3. Filtering & monitoring

Wishford schools recognise the importance of robust filtering and monitoring procedures as stipulated in KCSIE 2023.

Across the Wishford Group we utilise the services of Censornet Security to filter and monitor online usage onsite. Censornet filters content by category (see below), has a block and allow list (which allows us to add/remove access to specific websites) and can also filter by keyword allowing for an extremely targeted approach.

Examples of categories which are automatically filtered					
Abortion	Dating	Gambling	Intimate Apparel	Open HTTP Proxies	Spyware and Adware
Abuse	Drugs	Gaming	Keyloggers and Monitoring	Phishing and Other Frauds	Violence
Alcohol	Dynamic Anonymiser	Hacking	Malware Sites	Pornography	Weapons
Botnets	Discrimination	Hate/Racism	Marijuana	Profanity	
Cult/Occult	Eating Disorder	Illegal activity	Nudity	SPAM URLs	

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.

It should be noted that no filtering system is 100% effective – to allow educational use of the internet, not all available categories (advertising, image hosting etc.) can be blocked as most websites will fail to load. There may be times where a child can get to a site that the teacher would deem inappropriate – if this happens, the website should be reported to the IT Helpdesk by email with the subject title "Website Reclassification" to ensure that site is recategorized promptly.

VPNs (Virtual Private Networks) are freely available for most platforms. These can circumvent the school's filtering by creating a secure "tunnel" to an external server. Unfortunately, it is almost impossible to block the use of VPNs completely, as new providers appear regularly which use different techniques for bypassing the filtering. The only sure way to block these with our current equipment would also block many legitimate services that are needed by the school (due to login restrictions, it should not be possible for staff/pupils to install VPNs on school devices). Nevertheless, all VPNs should be reported to the IT helpdesk so they can be specifically blocked.

Alongside its filtering capabilities, Censornet monitors all internet usage on-site. All users have to login to the Wi-Fi and their usage (of school devices, systems and websites) is then automatically monitored. Staff and pupils should therefore not allow anyone else to use their login details and staff should log the number of the device being used by each individual pupil if a class uses a shared account.

Monitoring data can be reviewed on the Censornet administration portal. The DSL is responsible for overseeing the regular review of this information and acting accordingly. Termly governance visits and online safety committee meetings will also review procedures. The school will report any concerns immediately to the IT helpdesk and in line with other relevant policies including Bullying, Safeguarding and the Staff Code of Conduct.

In addition to the monitoring offered by Censornet, our online safety training and curriculum, alongside our Acceptable Use Agreement, offers a layered approach to keeping everyone safe online. Measures include:

- Regular training/guidance for staff/pupils on acceptable usage, including the use of personal devices.
- Regular updates for staff/pupils/parents on current online threats.
- Regular reminders for staff/pupils/parents on the procedures for reporting concerns.
- Visible use of IT on school site with pupil usage always being closely monitored by staff.

N.B. To ensure that secure (HTTPS) websites can continue to be monitored and filtered effectively, all devices will need to upload a security certificate. School owned/provided devices will have this loaded onto it automatically, but if staff or pupils require the use of the school internet on their own devices, they will need to load this certificate. Failure to do this will mean that most HTTPS websites will fail to display successfully. Instructions for installing the certificate on various different types of device (Apple iOS/MacOS, Windows, Android, Chromebook) are available in the "Useful Guides and Resources" section on SharePoint.

4. Technical Security Procedures

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

- users can only access data to which they have right of access.
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the data protection policy.
- Monitoring of usage is in place and data/systems are reviewed regularly.
- there is effective guidance and training for users.
- there are regular reviews and audits of the safety and security of school computer systems.
- there is oversight from senior leaders and these have impact on policy and practice.

Technical Security Overview

- The overall management of technical security will be the responsibility of the Group Head of Technology and the IT Team.
- The Group will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible.
- The School will ensure that policies and procedures are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities.
- 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.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- All users will have clearly defined access rights to school technical systems. Details of any elevated access rights available to user will be recorded by the Group Head of Technology and will be reviewed, at least annually.
- Users are responsible for the security of their username and password, must not allow other users to access the systems or Wi-Fi using their login details and must immediately report any suspicion or evidence that there has been a breach of security (see password section below).
- The Group Head of Technology 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs). School Staff will not install software without the express written permission of the Group Head of Technology.
- Mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).
- IT Department staff regularly monitor and record the activity of users of the school internet and users are made aware of this in the IT acceptable use agreement.
- Remote management tools can be used by IT staff to control school-supplied workstations and view users' activity.
- Any technical incident should be reported to the IT Helpdesk, who can escalate to the Group Head of Technology if required.
- Temporary access to school applications (Office 365 / PASS/3SYS / iSAMS) will be granted as per normal recruitment procedures – if this is required before a user starts their contract with the school, a pre-employment contract will need to be signed.

- Where available, guest Wi-Fi "Passes" can be granted by the school administration team without referring to HR, however, this only gives temporary internet access, not any access to the school systems.
- The downloading of executable files is blocked by the school internet filtering system
- Any device provided by the school is for school use only – family members/friends should not attempt to use the device, unless for the reason of helping a child (who is the assigned keeper of the device). Any personal use by the assigned keeper of the device is liable to be monitored.
- CDs/DVDs (whether audio/video or data) can only be used where the content is licensed for use in a commercial educational environment. USB memory sticks should not be used without prior authorisation from the IT department – the school provides all users with Microsoft Office 365 OneDrive for storing and moving data.
- The school infrastructure and individual workstations are protected by up to date antivirus software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent outside of the Group's Office 365 system over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

- All school networks and systems will be protected by secure passwords.
- All users (adults and students/pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the IT Helpdesk who will keep an up to date record of users and their usernames.
- Staff Password requirements:
    - Passwords must be at least 8 characters and include at least 3 of: lower case, upper case, number & non-alphabetical (e.g.! $, %).
    - Ideally, Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words (3 random words) that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
    - Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
    - Passwords must not include names or any other personal information about the user that might be known by others.
    - Passwords must be changed on first login to the system.
    - Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.
- Pupil Password requirements:
    - Prep schools will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class logons for shared devices (though increasingly children are using their own passwords to access programmes). Schools need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the acceptable use agreement (AUA). Use by students/pupils in this way should always be supervised and members of staff should never use a class log on for their own network/internet access. Outside of a class setting, pupils should use their own accounts – never a shared class login.
    - Records of learner usernames and passwords for students/pupils can be kept in a secure electronic form, but they must be securely kept when not required by the user.
    - Users will be required to change their password if it is compromised.
    - Students/pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Email Security: Some (phishing) emails can be scams or carry virus as malicious software; for example: as attachments or links. In order to avoid virus infection or data theft, our policy is always to inform staff to do the following:

- Abstain from opening attachments or clicking any links in the situations when its content is not well explained. *For example: if you receive an email attachment from someone you were not expecting or do not know.*
- Make sure to always check email addresses and names of senders. Lookout for inconsistencies & poorly written emails, misspelt names & domain names (*for example: microsfotonline.com*).
- Be careful with clickbait titles (for example offering prizes, advice, etc.).
- Undertake any cyber security training offered to staff.
- Staff should enable MFA (Multi Factor Authentication) for their school email account.

In case that staff are not sure if the email received, or any type of data is safe, they should always contact Wishford IT and forward the suspected email via Helpdesk (helpdesk@schooldomain.com) change to your school specific helpdesk email here.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.
- If there is only one top-level administrator in the group, an administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account. There should always be more than one administrator account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- Where user-controlled reset is not possible, passwords for new staff users, and replacement passwords for existing staff users will be allocated by the IT Helpdesk. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.
- Requests for password changes should be authenticated by the headteacher and/or the School Business Manager to ensure that the new password can only be passed to the genuine recipient.
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. (For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way. Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the acceptable use agreement
- Students/pupils will be made aware of the school's/college's password policy:
- in lessons (the school should describe how this will take place)
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The Group Head of Technology will ensure that full records are kept of:

- User IDs and requests for password changes (this will be logged in the helpdesk system)

- User logons (this is kept in Active Directory)
- Security incidents related to this policy

5. Education & Training

Pupils

Whilst filtering and monitoring are very important, their use must be balanced by educating our pupils to take a responsible approach. The education of our pupils in online safety is therefore an essential part of any Wishford 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.

Each school's Online Safety lead is responsible for ensuring a broad and thorough education in Online Safety for all pupils. The online safety curriculum must be outlined in either the school's Safeguarding, Curriculum or PSHE policy and clearly cross-reference in all three. As a minimum standard, the curriculum overview should include coverage of the following:

- How the online safety curriculum has good coverage of the key areas outlined in official guidance, namely:
    - DfE Teaching Online Safety in Schools
    - Education for a Connected Word Framework
    - SWGfL Project Evolve – online safety curriculum programme and resources
- An overview of what is taught, how it is taught and by whom.
- How the school deals with topics such as copyright, social media training for pupils and Prevent training (as part of the school's responsibility in line with the Counter Terrorism and Securities Act 2015).
- The risks involved in sharing images and personal details online and strategies to deal with inappropriate contact/communication.
- Wider contributions to online safety awareness, e.g. safer internet day, guest speakers, assemblies/house competitions etc…
- The DSL's procedures for monitoring Censornet.
- The role of the online safety committee (staff) in developing the provision.
- The role of the school council (or other group) in developing the provision, raising awareness and sharing experiences.
- Pupil training on Acceptable Use.
- Channels through which pupils can report any online safety concerns.
- The approach to reviewing and updating the provision in line with the latest trends and more current concerns.

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. Again, each school's approach to parental engagement should be outlined within their online safety curriculum overview. Activities might include:

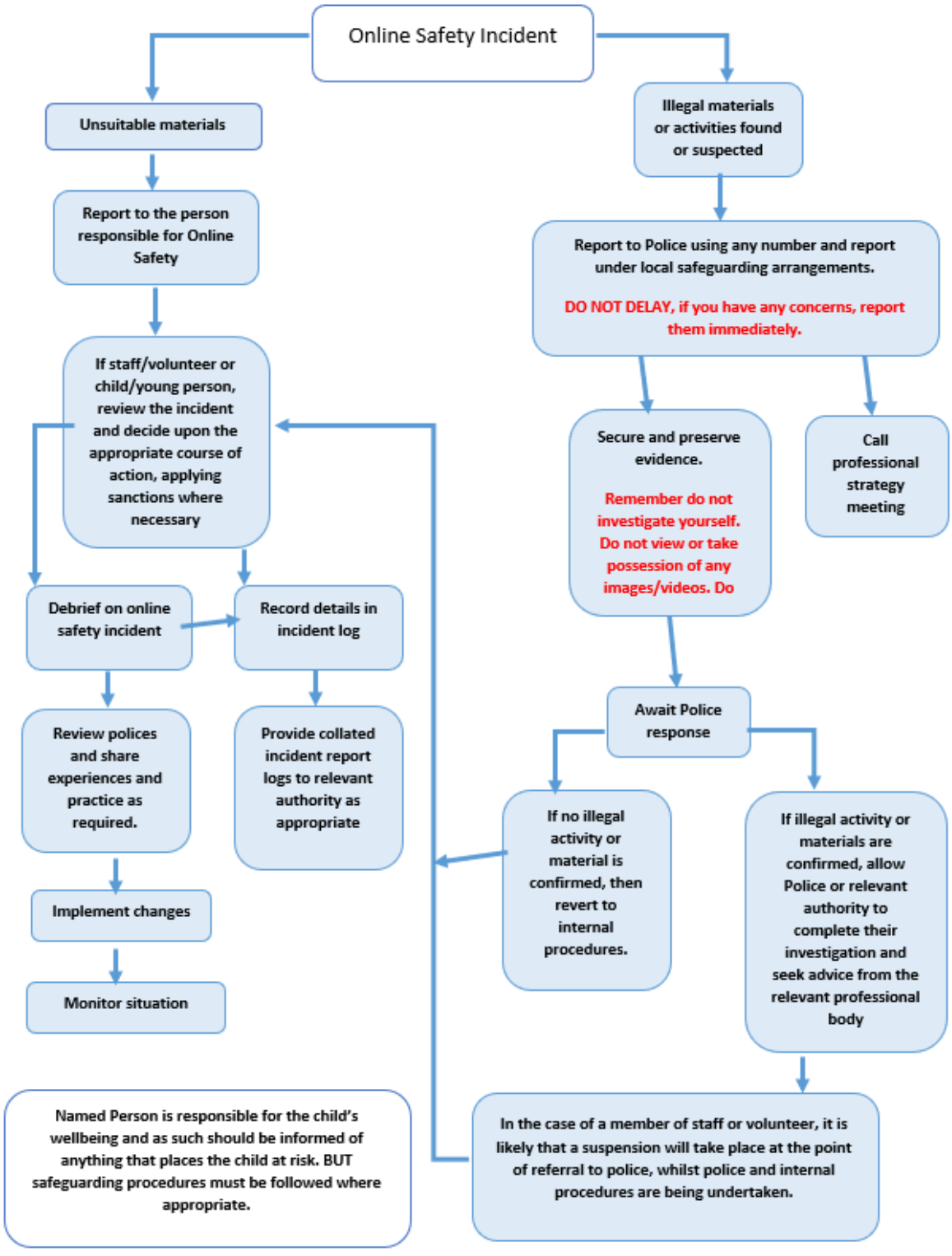
- Parent workshops
- Letters, newsletters, web site, Learning Platforms.
- High profile events/campaigns e.g. Safer Internet Day.
- Channels through which parents can report any online safety concerns (internal and external).
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers, NOS Parent APP.

Staff/Volunteers

All staff and volunteers across Wishford Schools must understand the inherent dangers of the online world and be prepared to support and guide our pupils. Each school should outline how they support and train their staff/volunteers within their online safety curriculum overview. Minimum standard guidance is as follows:

- Formal annual training including:
    - policy updates.
    - coverage of the reporting/monitoring systems and staff responsibilities.
    - Coverage of appendix 1: Technical Security and the IT Acceptable Use Policy – staff should sign an agreement.
    - coverage of the staff code of conduct in relation to online activity/acceptable use and the expectation that staff act as role models.
    - Best practice for safe usage during lessons, e.g. visible usage and pre-checked internet sites/content.
    - Use of TES develop.
- Induction training for new staff (especially if they miss the annual training).
- Communication from/to the online safety committee, including methods for updating staff on up to date issues/risks/pupil usage.
- Channels through which staff can report any online safety concerns (internal and external).
- Low level concerns/Whistleblowing policies and staff responsibilities.

Appendix 1: Dealing with an Online Safety Incident



Appendix 2: Exemplar Online Safety Incident Log

Reporting Log Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix 3 - Legislation

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.
- School/academies may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

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

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

The Data Protection Act 2018

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.
- All data subjects have the right to:
- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure

- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

Establish the facts;

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education
- These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012

Requires schools to publish certain information on its website:

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

Serious Crime Act 2015

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

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

Appendix 4 - Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

DfE Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework