Online Safety Policy

The Stour Federation

Date of publication: April 2022 Review Date: September 2023

Contents

1. DEVELOPMENT/MONITORING/REVIEW OF THIS POLICY

This Online Safety Policy has been developed by the pupils, parents and community committees made up of:

- Executive Headteacher.
- Heads of School.
- Staff.
- Local Academy Councils (including Online Safety Governors).
- Parents and Carers.

Consultation with The Stour Federation community has taken place through a range of formal and informal meetings:

- Staff Meetings and INSET.
- Governors Meetings.
- School Newsletters.
- Parents Information Evenings/Workshops.

Schedule for Development/Monitoring/Review

This Online Safety Policy was approved by the Trust Board of Directors and Local Academy Councils on:	*April 2022*
The implementation of this Online Safety Policy will be monitored by the:	*Leadership Team* *Online Safety Coordinator* *Computing Curriculum Team* *Online Safety Governor* *Pupils, Parents and Community* *Local Academy Councils*
Monitoring will take place at regular intervals:	*Autumn Term - annually*
The Local Academy Councils in The Stour Federation will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Summer Governors Meeting*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2023*
Should serious Online Safety incidents take place, the following external persons/agencies should be informed:	*ICT Development Service* *Warwickshire Police* *Warwickshire Safeguarding* *Education Lead* *LADO*

The schools will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited and filtering).

- Internal monitoring data for network activity.
- Surveys/questionnaires of pupils, parents and staff.

Scope of the Policy
This policy applies to all members of The Stour Federation (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school/academy digital technology systems, both in and out of each school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Each 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.

2. ROLES AND RESPONSIBILITIES

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the schools.

Trust Board of Directors/Local Academy Councils
Directors 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 Board receiving regular information about Online Safety incidents and monitoring reports. A member of the Local Academy Councils has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Lead.
- Attendance at Online Safety Group meetings.
- Regular monitoring of Online Safety incident logs.
- Regular monitoring of filtering/change control logs.
- Reporting to relevant Boards/Local Academy Councils.

Executive Headteacher and Heads of School
The Executive Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community; as Online Safety Lead, the Executive Headteacher also has a day to day responsibility for Online Safety.

The Executive Headteacher and Heads of School should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse”..

The Executive Headteacher and Heads of School 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 those colleagues who take on important monitoring roles

.

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

Online Safety Lead

The Executive Headteacher (EPICT Online Safety Certificate) is the Online Safety Lead and is responsible for:

- Taking day-to-day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Providing training and advice for staff.
- Liaising with the Local Authority.
- Liaising with technical staff.
- Receiving reports of Online Safety incidents and creating a log of incidents to inform future Online Safety developments.
- Meeting regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attending relevant meetings/Local Academy Council meetings.
- Reporting regularly to the Leadership Team.

Network Management

The Stour Federation has a managed ICT service provided by Warwickshire ICT Development Service. It is the responsibility of each school to ensure that the managed service provider carries out all the Online Safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of The Stour Federation Online Safety Policy and procedures.

Warwickshire ICTDS are responsible for ensuring:

- That each school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That each school meets required online safety technical requirements and any guidance that may apply.
- That users may only access the networks and devices through a properly-enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its 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.
- The use of the network, internet, WeLearn365, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Executive Headteacher for investigation, possible action and sanction.
- That monitoring software and systems are implemented and updated as agreed in The Stour Federation policies.

Teaching and Non-Teaching Staff

Are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of the current Stour Federation Partnership Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement and Staff Behaviour Policy (Code of Conduct).
- They report any suspected misuse or problem to the Executive Headteacher for investigation, possible action and sanction.
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems.
- Online Safety issues are embedded in all aspects of the curriculum and other activities - teachers should plan for each school to embed 'Education for a Connected World' into their planned curriculum.
- Pupils understand and follow the Online Safety Policy and Acceptable Use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Leads (DSLs)
The DSLs at each school 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 online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Online bullying.

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.

Pupils
- Are responsible for using their school's digital technology systems in accordance with the Pupil Acceptable Use policy.
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile and wearable devices and digital cameras. They should also know and understand policies on the taking and 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 Stour Federation'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 as the vast majority of online safety issues arise out of school. It is the responsibility of parents to be actively involved and check chats, feeds gaming conversations regularly, as well as keeping up to date with new apps, games and sites. Each school will take every opportunity to help parents understand these issues and their responsibilities through parents' evenings, newsletters, letters, the school website, Twitter, Seesaw and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support their 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 school website/Seesaw/WeLearn365.
- Their children's personal devices in the school (where this is allowed).

Community users

Community Users, who access school systems or programs as part of the wider school provision, will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems.

3. POLICY STATEMENTS

Education – Pupils

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

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

- A planned Online Safety curriculum should be provided as part of Computing and PSHE lessons, as well as part of the delivery of other curriculum lessons involving online content/resources.
- The Online Safety curriculum should be regularly revisited - each school should make use of the 'Education for a Connected World Framework' and 'SWGfL Project Evolve', to deliver their Online Safety curriculum programme of study.
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and where appropriate, suggest age-appropriate search engines such as Kiddle/Google SafeSearch.
- It is accepted that from time to time, for good educational reasons, pupils 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 Computing Lead, Head of School or Executive Headteacher can request that ICTDS temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Some parents and carers may 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 and 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.

Each school in The Stour Federation will therefore seek to provide information and awareness to parents and carers through:

- *C*urriculum activities.
- Letters, newsletters, school website, Seesaw, Twitter.
- Parents/carers information evening and workshops.
- High profile events/campaigns e.g. Safer Internet Day; Anti-Bullying Week.
- Reference to the relevant websites and publications such as
    - *o* swgfl.org.uk,
    - *o* www.saferinternet.org.uk/,
    - *o* http://www.childnet.com/parents-and-carers,
    - *o* www.internetmatters.org

Education – The Wider Community

Each school in The Stour Federation may provide opportunities for local community groups to gain from the school's Online Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and Online Safety.
- Online Safety messages targeted towards grandparents and other relatives, as well as parents.
- Each school's website will provide Online Safety information for the wider community.
- Sharing their Online Safety expertise/good practice with other local schools.
- Supporting community groups e.g. Early Years settings, childminders and voluntary organisations, to enhance their Online Safety provision.

Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world. In combination with our PSHE curriculum (e.g. Protective Behaviours), Online Safety lessons will also promote resilience and critical thinking when accessing the online world and ensure pupils build healthy online relationships and engage positively with online technologies. As a result, it is our intention that our pupils will become confident and responsible digital citizens.

Education and 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 e.g. through the use of Online Safety BOOST online webinar training; attendance at the annual ICTDS Online Safety Conference. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within their performance management process.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand The Stour Federation Online Safety Policy and Acceptable Use Agreements.
- The Executive Headteacher will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and on INSET days.
- The Executive Headteacher will provide advice/guidance/training to individuals as required.

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

- Attendance at training provided by the Local Authority/MAT/National Governors Association or other relevant organisation (e.g. SWGfL).
- Participation in information sessions for staff or parents, including assemblies and lessons.

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

- School ICT systems will be managed in ways that ensure that each school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of each school's technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.

- All users will have clearly defined access rights to school ICT systems and devices.
- All users will be provided with a username and secure password by ICTDS who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password when prompted, in accordance with LA password policy.
- The network manager and administrator passwords for each school's ICT system must also be available to the Executive Headteacher and Heads of School and kept in a secure place.
- The Executive Headteacher 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.)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Each school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils, etc...)
- The Online Safety Lead regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place (to be described) for users to report any actual/potential technical incident or security breach to the Executive Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. Each school's infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that staff are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/download executable files and install programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including Bring Your Own Device (BYOD))

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include Seesaw, WeLearn365, Google Workspace and other cloud based services for email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and interrelated to other relevant school policies including, but not limited to, the Child Protection and

Safeguarding Policy; Anti-Bullying Policy; Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

Each school has a set of clear expectations and responsibilities for all users:

- The Stour Federation Acceptable Use Agreements for staff and pupils will give consideration to the use of mobile technologies
- The Stour Federation schools allow:

School Devices				Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	Google Workspace	No
Internet only				No	Yes	Yes

Use of Digital and Video Images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press - parents will consent to the use of these photographs in each individual circumstance and a central record kept (school GDPR log).
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their own children at school events for

[1]

their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow The Stour Federation's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on authorised equipment.
- 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 according to parent/carer GDPR consent given 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 Stour Federation must ensure that:

- It has a Data Protection Policy.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (Warwickshire Legal Services) and Data Protection Lead (Executive Headteacher) who has a high level of understanding of data protection law and is free from any conflict of interest. The Trust 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 is accurate and up to date where this is necessary for the purpose it is processed for.
- It has systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.

- It provides staff, parents, governors and volunteers with information about how the school looks after their data and what their rights are in clear Privacy Notices.
- 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 and 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 a managed service, insured and regularly checked. Patches and other security essential updates are applied promptly (by ICTDS) 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.
- 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:

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

Staff must ensure that they:

- At all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse (referring to Information Security Policy, Data Protection Policy and GDPR privacy notices).
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Can help data subjects understand their rights and know how to handle a request, whether verbal or written and they 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 Trust 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.

4. COMMUNICATIONS

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

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

When using communication technologies, the Trust considers the following as good practice:

- The official WeLearn365 email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the WeLearn365 email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report to the nominated person – in accordance with The Stour Federation policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school/academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will be provided with individual school email addresses for educational use.
- Students/pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school websites and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies, MATs 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 Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The Stour Federation provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to 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, The Stour Federation, or local authority.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

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

Personal Use:

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

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school/Trust.
- The school/Trust should effectively respond to social media comments made by others according to a defined policy or process. Each school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

5. DEALING WITH UNSUITABLE/INAPPROPRIATE ACTIVITIES

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The Stour Federation 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/ outside school when using school equipment or systems. The Stour Federation policy restricts usage as follows:

User Actions 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:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✔
Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003					✔
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Sexual Offences Act 2008					✔
Criminally racist material in the UK - to stir up religious hatred (or hatred on any grounds of sexual orientation) - contrary to the Public Order Act 1986					✔
Pornography				✔	
Promotion of any kind of discrimination				✔	
Threatening behaviour, including promotion of physical violence or mental harm				✔	
Promotion of extremism or terrorism				✔	
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				✔	
Using school systems to run a private business				✔	
Using systems, applications,				✔	

websites or other mechanisms that bypass the filtering or other safeguards exploited by the school					
Infringing copyright				✔	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				✔	
Creating or propagating computer viruses or other harmful files				✔	
Unfair usage (downloading/uploading large files that hinder others in their use of the Internet)				✔	
Online gaming (educational	✔				
Online gaming (non-educational)		✔			
Online gambling				✔	
Online shopping/commerce		✔			
File sharing	✔				
Use of social media			✔		
Use of messaging apps			✔		
Use of video broadcasting e.g.Youtube	✔				
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information					✔

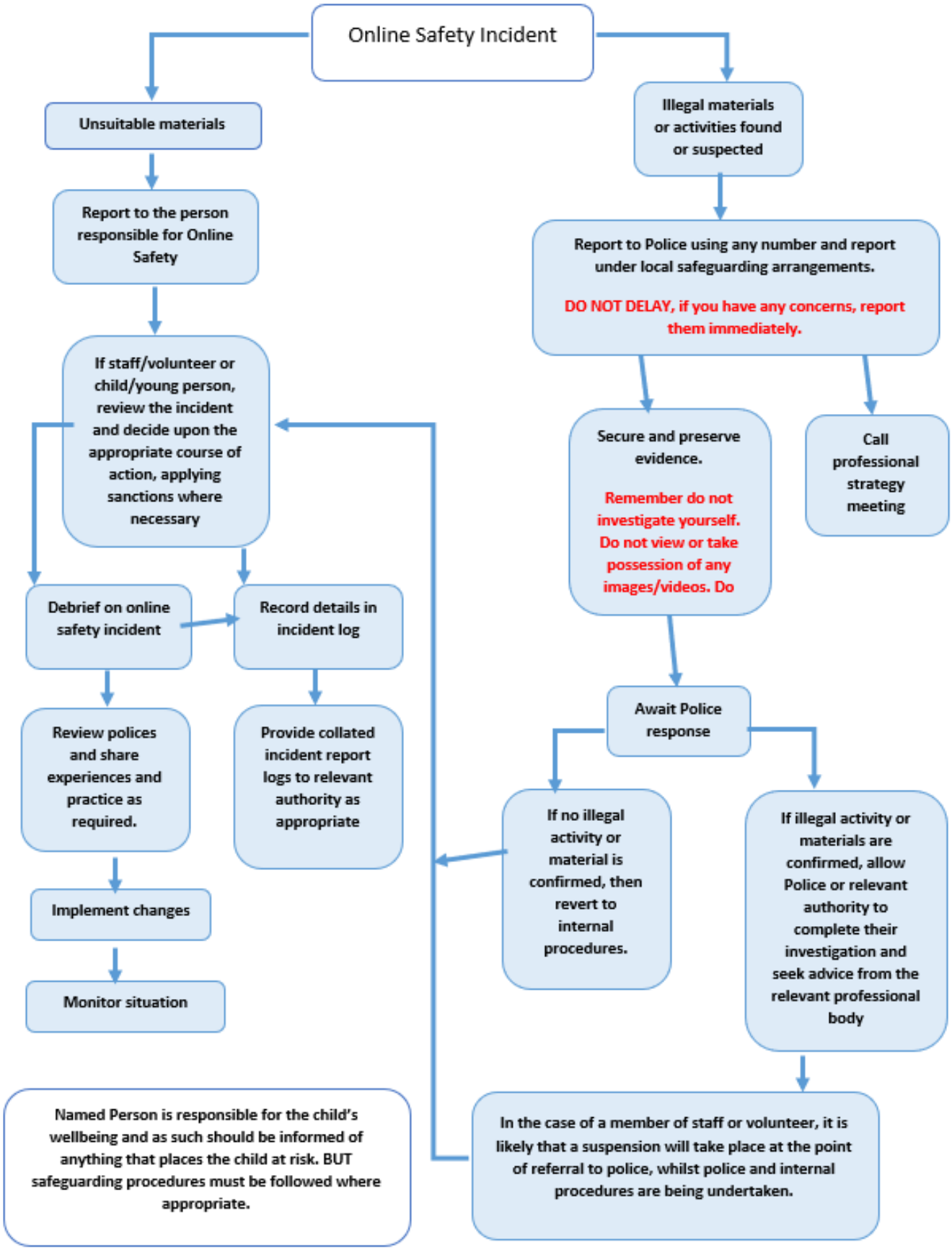
(e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

6. 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.


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

7. OTHER INCIDENTS

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

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

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

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

8. SCHOOL ACTIONS AND SANCTIONS

It is more likely that each school in The Stour Federation 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

Pupil Incidents	Refer to class teacher	Refer to Online Safety Coordinator	Refer to Executive Head or Head of School	Refer to police	Refer to ICTDS for action re filtering/security etc...	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. 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 use of mobile phone/ digital camera/ other mobile device		✔	✔			✔	✔	✔	
Unauthorised use of social media/ messaging apps/ personal email		✔	✔		✔	✔	✔	✔	
Unauthorised downloading or uploading of files		✔	✔		✔	✔	✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔					✔	✔	
Attempting to access or accessing the school network, using another pupil's account		✔	✔			✔	✔	✔	
Attempting to access or		✔	✔		✔	✔	✔		✔

accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users		✔	✔		✔	✔	✔		✔
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✔	✔			✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions		✔	✔			✔	✔		✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✔	✔			✔	✔		✔
Using proxy sites or other means to subvert the school's filtering system		✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material and failing to report the incident		✔	✔		✔	✔	✔		
Deliberately accessing or trying to access offensive or pornographic material		✔	✔	✔	✔	✔	✔		✔
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✔	✔	✔		✔	✔		

Actions/Sanctions

Staff Incidents	Refer to Executive Headteacher of Head of School	Refer to Local Authority/ Governors/ HR	Refer to police	Refer to ICTDS for action re filtering/security etc...	Warning	Possible disciplinary action	Possible suspension/ dismissal
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities)	✔	✔	✔			✔	✔
Inappropriate personal use of internet/ social media/ email	✔			✔	✔	✔	
Unauthorised downloading or uploading of files	✔			✔	✔		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✔			✔	✔		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✔				✔	✔	
Deliberate actions to breach data protection or network security rules	✔	✔		✔		✔	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✔		✔	✔		✔	✔
Sending an email, text or	✔	✔				✔	

message that is regarded as offensive, harassment or of a bullying nature							
Using personal email/ social networking/ instant messaging/ text messaging to carry out digital communications with pupils	✔	✔		✔		✔	✔
Actions which could compromise the staff member's professional standing	✔	✔			✔	✔	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔	✔			✔	✔	
Using proxy sites or other means to subvert the school's filtering system	✔	✔		✔		✔	
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔	✔	✔	✔		
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔	✔		✔	✔
Breaching copyright or licensing regulation	✔				✔		
Continued infringements of the above, following previous warnings or sanctions	✔	✔				✔	

9. ACKNOWLEDGEMENTS

This policy is based on the template policies by SWGfL who would like to acknowledge the contribution of a wide range of individuals and organisations whose policies, documents, advice

and guidance have contributed to the development of the Online Safety Policy templates and of the 360 degree safe Online Safety self-review tool.

APPENDICES

SUPPORTING DOCUMENTS/POLICIES

Keeping Children Safe In Education 2021

Data Protection Policy 2021

Information Security Policy 2021

Privacy Notice - Parents and Pupils 2021

Staff Privacy Notice 2021

Privacy Notice - Governance 2021

Acceptable User Policy

Staff Chromebook Agreement

ICTDS Filtering & Monitoring Policy

Staff Behaviour Policy

Guest Acceptable Use Policy

LEGISLATION

Schools/academies 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 an 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 helpline 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 TradeMarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks 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 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.

For further guidance or support please contact the Revenge Porn Helpline

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

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

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 Framework -

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

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour -

http://www.scotland.gov.uk/Publications/2013/03/7388

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

NHS - Caldicott Principles (information that must be released)

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

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
ICTDS	ICT Development Service
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.