Stowmarket High School

THE FUTURE · OUR BUSINESS

ONLINE SAFETY POLICY

This policy is reviewed bi-annually

Policy Reviewed	October 2023
Next Review Due	October 2025

Index

Appendices

1. **Online Safety Flow Chart**
2. **Acceptable use agreement for staff**
3. **Acceptable use agreement for students**
4. **Online resources for parents and staff**

Introduction

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is the duty of Stowmarket High School to ensure that young people are protected from potential harm both within and beyond our school.
This policy aims to explain how students can be a part of these safeguarding procedures. It also details how students are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term Online Safety is used:

- to encompass the safe use of all technologies in order to protect all from potential and known risks.
- to emphasise the need to educate staff and students about the pros and cons of using new technologies both within and outside school.
- to provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- to ensure adults are clear about procedures for misuse of any technologies.

Roles and Responsibilities

The Local School Committee/ Head teacher

It is the overall responsibility of the Headteacher to ensure that there is an overview of Online Safety as part of the wider remit of safeguarding across Stowmarket High School with further responsibilities as follows:

- The Headteacher has designated an Online Safety Lead to take responsibility for ensuring Online Safety is addressed and safe practice promoted amongst students in order to establish a safe ICT learning environment.
- The Keeping Children Safe in Education (2023) document highlights that the Designated Safeguarding Lead (Andy McLellan) is the person responsible to ensure that staff complete training focusing on students using the internet safely. Staff will

be trained to understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

- The Headteacher, with Directors of IT, Andrew Wright, and subject lead for PSHE, Claire Ferguson, has responsibility for promoting Online Safety across the curriculum.
- The School Committee will be informed of the progress of or any updates to the Online Safety curriculum by the Online Safety Lead, Andy McLellan, and ensure the School Improvement Board know how this relates to safeguarding. It is the responsibility of School Committee to ensure that all safeguarding guidance and practices are embedded.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police where appropriate or involving parents/carers.
- The School Improvement Board should ensure that children are taught about safeguarding, including online safety, and recognise that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed.

School Online Safety Lead and Network Manager

It is the role of the Online Safety Lead working with the Director of IT to:

- Appreciate the importance of Online Safety within Stowmarket High School and to recognise the duty of care to ensure the safety of students and staff.
- Establish and maintain a safe IT learning environment within our school.
- Ensure that Acceptable Use Agreements, for both staff and students, are reviewed periodically, with up-to-date information and that training is available for our staff to teach Online Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for our staff and students, in the initial set up of school IT equipment, including an appropriate level of security protection procedures.
- Report issues.
- Liaise with the PSHE, Safeguarding and IT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training according to new and emerging technologies so that the correct Online Safety information can be taught or adhered to.
- Ensure transparent monitoring of the Internet and online technologies.
- Keep a log of incidents to help inform future development and safeguarding, where risks can be identified. All concerns should be logged and recorded on my concern.
- Ensure there is appropriate and up-to-date anti-virus software and anti-spyware on our school IT equipment and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on our school IT equipment and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised. Refer to the Managing Allegations Procedure (Fig 1), LSCB (Suffolk), for

dealing with any issues arising from indecent or pornographic/child abuse images sent/received.

- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher.

Staff or Adults

It is the responsibility of all adults within Stowmarket High School to:

- Ensure that they know who the Designated safeguarding Lead and their deputies for Safeguarding are within school so that any misuse or incidents can be reported which involve a child. Andy McLellan is the Designated Safeguarding Lead. Amy Underwood is the School Improvement Board member in charge of Safeguarding.
- Where an allegation is made against a member of staff, it should be reported immediately to the Head teacher/Senior Designated Persons. In the event of an allegation made against the Headteacher, the Chair of the School Improvement Board must be informed immediately.
- Be familiar with the Anti-Bullying, child-to-child Abuse, Behaviour for Conduct, Whistleblowing and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Head teacher/Senior Designated Persons immediately.
- Alert the Online Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that students are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. They should know what to do in the event of an incident.
- Be up-to-date with Online Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Adhere to the Acceptable Use Agreement within and beyond the school, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 2018. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended or unlocked when they or another user is logged in.
- Report accidental access to inappropriate materials to the Online Safety Lead and Network Manager in order that inappropriate sites are blocked where possible.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of personally directed bullying or other inappropriate behaviour via the Internet or other technologies to the Head teacher/Senior Designated Persons.
- Ensure that all concerns about sexual violence and/or harassment, both online and offline, are reported appropriately, with information recorded on 'My Concern'.

Students

Children and young people should be:

- Involved in the review of Acceptable Use Agreement through the school, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Agreement.

- Taught to use the internet in a safe and responsible manner through IT and PSHE.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand.
- 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.

By the end of secondary school pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all context, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and to report, or find support, if they have been affected by those behaviours.

Staff training

School will ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online safety, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is a wealth of information available to support schools and parents to keep children safe online. Appendix 4 is not an exhaustive list but should provide a useful starting point.

Appropriate and Inappropriate Use by Staff, Adults and Students

Acceptable Use Agreement for staff

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. Staff will be asked to sign a digital Acceptable Use

Agreement at the start of the new school year, or at the beginning of their employment if they join part way through the school year.

When accessing the school network or using school IT equipment from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for our staff to that of our students so that an example of good practice can be established.

In the Event of Inappropriate Use
If a member of our staff is believed to deliberately misuse the internet or school network in an abusive or illegal manner, a report must be made to the Head teacher/Senior Designated Persons immediately and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Acceptable Use Agreement for students
Acceptable Use Agreement for students and parents/carers are outlined in the Appendices, a copy of which will be available on the school website. These detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. Students will sign an agreement at the start of each academic year to remind them of the online expectations. The agreements are there for students to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is acceptable when using school emails or school internet, or understanding what action to take should there be sighting of unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The school should encourage parents/carers to support the agreement with their child. This is also intended to provide support and information to parents/carers when students may be using the internet beyond school.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.
File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the school network or equipment in or beyond Stowmarket High School.

In the Event of Inappropriate Use
Should a student be found to misuse the online facilities whilst at school, the following consequences should occur:

- A letter sent home to parents/carers explaining the reason for suspending the student's use of the internet for a period of time.
- Serious incidents of misuse may lead to exclusion and/or police involvement if it is believed a criminal offence may have occurred.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action. Where a child

or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the CEOP report abuse button to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.
Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

The Curriculum and Tools for Learning

Opportunities to teach safeguarding

Stowmarket High School will ensure that children are taught about safeguarding, including online safety. As a school we consider this as part of providing a broad and balanced curriculum.

Internet Use

Stowmarket High School will endeavour to teach students how to use the Internet safely and responsibly. They should be taught, through IT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave Year 11:

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.
- How to judge what they see online.
- How to recognise techniques used for persuasion.
- Identifying online risks.

Students should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.

- School/education setting or other establishment.
- Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school/education setting or other establishment.
- Identifying information, e.g. I am number 8 in the school football team.

Pupils with Additional Learning Needs
The school will strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

Photographs
Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'.
Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy.
Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

School Website
The uploading of images to the school website is subject to the same acceptable agreement as uploading to any personal online space. Permission is sought from the parent/carer prior to the uploading of any images. We will consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

External Websites
In the event that a member of staff finds themselves or another adult on an external website, such as Facebook, Instagram, Snapchat, Twitter, Spotted in or 'Rate My Teacher', as a victim, they are encouraged to report incidents to the Head teacher.

E-mail Use
Stowmarket High School has e-mail addresses for students to use as part of their entitlement to being able to understand different ways of communicating and using IT to share and present information in different forms. Individual email accounts can be traced if there is an incident of misuse. Staff and students should use their school issued email addresses for any communication between home and school.

Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with young people is to communicate about who they may be talking to and assess risks together.

Mobile Phones and Other Emerging Technologies
Stowmarket High School carefully considers how the use of mobile and smart technologies can be used as a teaching and learning tool within the curriculum with the following areas of concern to be taken into consideration:

- Inappropriate or bullying text messages.
- Images or video taken of adults or peers without permission being sought.
- The videoing of violent or abusive acts towards a child, young person or adult which is often distributed.
- Nudes and semi-nudes - the sending of suggestive or sexually explicit personal images via mobile phones.
- Wireless Internet access, which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

Personal Mobile Devices
Staff should be allowed to bring in personal mobile phones or devices for their own use but **must not use personal numbers to contact children and young people under any circumstances.** In circumstances where it is necessary for staff to contact parents using their own devices the number must be hidden within the phone settings or by using 141 at the start of the number.

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Staff should be aware that games consoles and other such systems have Internet access which may not include filtering.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

Video and Photographs
The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. Permission must be sought prior to any uploading of images to check for inappropriate content.
The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.
Photographs/images used to identify children and young people in a forum or using Instant Messaging within the learning platform should be representative of the child rather than of the child e.g. an avatar.
Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to our school, other education setting or establishment website. Photographs should only ever include the child's first name although safeguarding guidance states either a child's name or a photograph but not both.
Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. Stowmarket High School will need to decide how photographs will be used, including where they will be stored and when they will be deleted. It is current practice by external media such as local and national newspapers to include the full name of children and young people in their

publications. Photographs of students should only be used after permission has been given by a parent/carer.

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of Stowmarket High School. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where students (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

In extreme circumstances, for example prolonged school closures, it may be necessary to conduct lessons via video-conferencing. Staff must use Microsoft Teams to do so, only using school based emails for both students and staff involved and approval should be sought from the head teacher before doing so.

Managing Social Networking and Other Web 2.0 Technologies

Social networking sites are a leading method of communication proving popular amongst both adults and young people alike. The service offers users both a public and private space through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed. With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published.

In response to this issue the following measures should be put in place:

- Stowmarket High School will control access to social networking sites through existing filtering systems.
- Students are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school/education setting or other establishment name, groups or clubs attended, IM and email address or full names of friends).
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school/education setting or other establishment uniform).
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.

- Social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the anti-bullying policy, to be followed.
- Students are advised to disable location sharing on social media platforms.

Social Networking Advice for Staff

Social networking outside of work hours, on non-school-issue equipment, is the personal choice of all Stowmarket High School staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Head teacher authorised systems (e.g. school email account for homework purposes). There may be extenuating circumstances if, for example, the member of staff is related to the student. It is advised that staff make these circumstances clear when signing the acceptable uses agreement (appendix 2).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a **professional** level. Some schools have set up accounts on Facebook to manage and monitor public and pupil communications through designated members of staff. Other such professional social networking tools include EdModo or Virtual Learning Environments such as Moodle which contain similar features.

Filters and monitoring

Stowmarket High School will be doing all that they reasonably can to limit children's exposure to the risks from the school's IT system. As part of this process, the school has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, the school has considered the age range of the pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

Whilst filtering and monitoring are an important part of the online safety picture that the school has considered, it is only one part. The school has considered a whole school approach to online safety, which includes a clear policy on the use of mobile technology in

the school. Many children have unlimited and unrestricted access to the internet via 3G, 4G of 5G technology in particular and the school will provide education via PSHE, IT and focussed assemblies to educate the pupils in the ways that this technology should be used, both in and out of school.

Whilst it is essential that the school ensure that appropriate filters and monitoring systems are in place, we understand that "over blocking" can lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Tools for Bypassing Filtering
Web proxies are probably the most popular and successful ways for students to bypass Internet filters today, where young people can access the Internet. Web proxies also provide an anonymous route through filtering safeguards in existence on networked facilities, allowing users to navigate through potentially harmful or inappropriate content.

A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which material can be viewed. The most common use of this tool amongst students is to access social networking features, gaming websites or information of an adult nature- all of which is blocked through the school's filtering system.

Due to the ever evolving nature of this bypassing tool, and the tens of thousands of websites offering set-up guidance, this is not an issue that can be solved overnight. It is advisable to refer to it within the Acceptable Use Agreement for both staff and pupils as an effective way for our school to manage the problem.

Students and staff are forbidden to use any technology designed tocircumvent, avoid or bypass any school/education setting or other establishment security controls (including internet filters, antivirus solutions or firewalls) as stated in the Acceptable Use Agreement. Violation of this rule will result in disciplinary or in some circumstances legal action.
It is worth noting however, that block banning of student's IT or internet access can be severely disruptive to learning across the curriculum and can also affect lesson planning and should only be applied in the most serious breaches.

Parents' – Roles
Every pupil should receive a copy of the Acceptable Use Agreement on first-time entry to the school which needs to be read with the parent/carer, signed and returned to school, confirming both an understanding and acceptance of the agreement. The signed documents will be scanned and held digitally by the Online Safety Lead.
It should be expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes

- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school will ensure that:

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

Communications

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

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones	✓				✓			
Use of mobile phones in lessons		✓					✓	
Use of mobile phones in social time	✓				✓			
Taking photos on mobile phones / cameras		✓					✓	
Use of other mobile devices e.g. tablets, gaming devices	✓						✓	
Use of personal email addresses in school – to access school related materials such as ShowMyHomework		✓				✓		
Use of school email for personal emails				✓				✓
Use of messaging apps		✓				✓		
Use of social media		✓				✓		
Use of blogs		✓				✓		

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students will be provided with individual school email addresses for educational use.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Social Media

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as YouTube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying, child-on-child abuse and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

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

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

Staff

School staff should ensure that:

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

When official school 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 a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or

impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Pupil/Students

- Staff are not permitted to follow or engage with current or prior students of the school on any personal social media network account, where extenuating circumstances apply such as being related to the pupil, these should be reported to the head teacher/Online Safety Lead.
- The school's education programme should enable the pupils/students to be safe and responsible users of social media.
- Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments made about the school will be resolved by the use of the school's behaviour policy. Any offensive or inappropriate comments made about staff will be resolved by the use of the school's behaviour policy. Unlawful behaviour, such as imitating a member of staff online will also be dealt with using the school's behaviour policy and, if necessary, be reported to the police.

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 by the School Liaison officer.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Monitoring of School Accounts

School accounts must be monitored regularly and frequently (preferably 5 days a week, within school working hours). Any comments, queries or complaints made through those accounts must be responded to within 48 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

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.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school safeguarding protocols.

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

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 Criminal Justice and Immigration Act 2008					✓
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
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 employed by the school				✓	
Infringing copyright					✓
Revealing or publicising confidential or proprietary information (egg 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 hinders others in their use of the internet)				✓	

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts Dos and Don'ts

The Dos

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties

- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible.

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Links to Other Policies – Safeguarding, Behaviour and Anti-Bullying Policies

Please refer to these policies for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs.
All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all IT and PSHE materials for children and young people and their parents/carers. People should not treat online behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which is reflected within our Behaviour for Learning and Anti-bullying policies as it is only the tools and technologies that change, not the behaviour of young people and adults.

Managing Allegations against Adults Who Work With Children and Young People

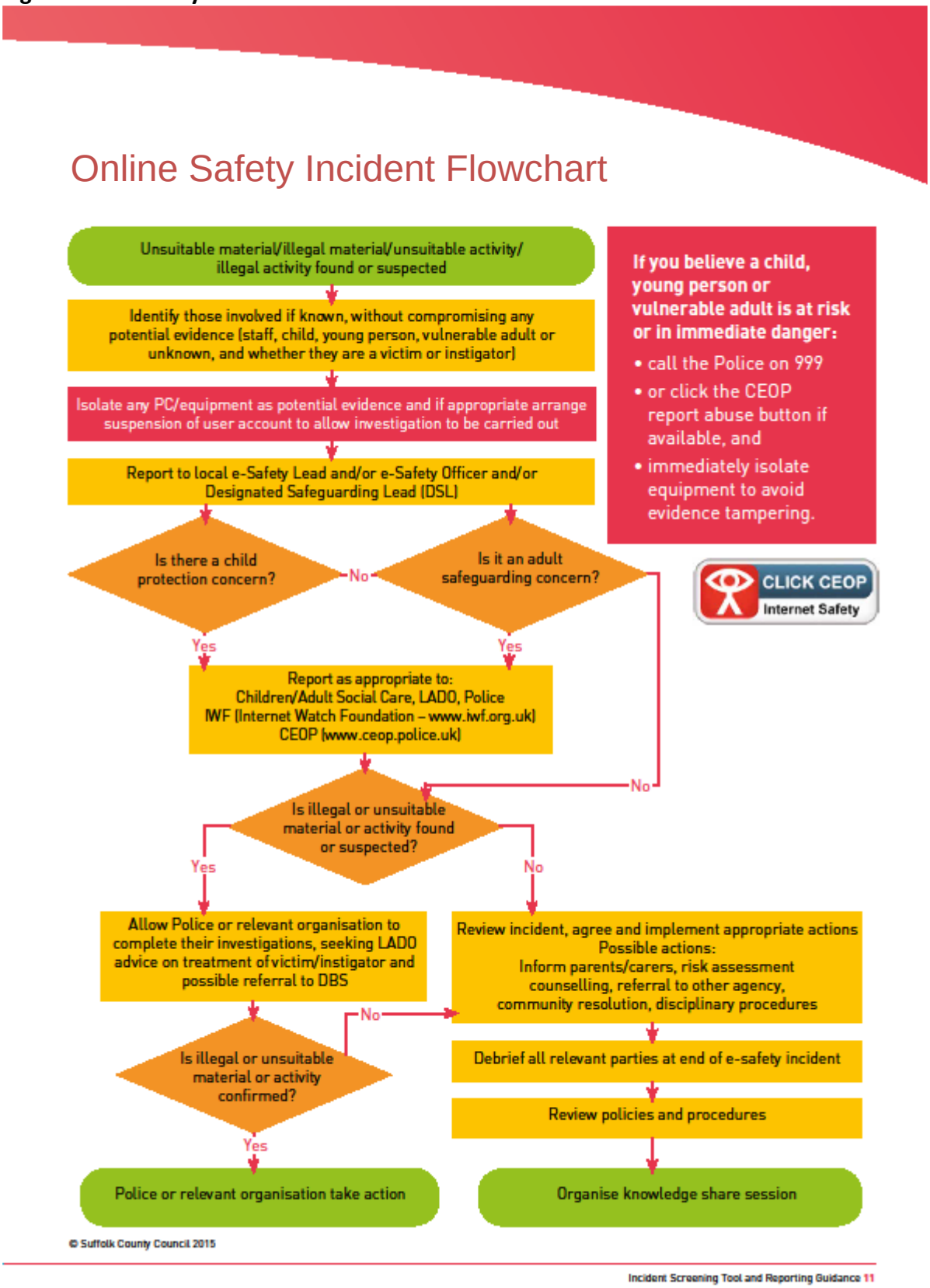
Please refer to the Managing Allegation Procedure (Fig 1), in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegations of misuse or misconduct being made by any member of staff or child about a member of staff.
Allegations made against a member of staff should be reported to the Senior Designated Persons for safeguarding immediately. In the event of an allegation being made against the Head teacher, the School Committee should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:

The Local Authority has designated officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies. Our LADO is Simon Hope , email address: simon.hope@suffolk.gov.uk

Appendix 1

Fig 1: Online Safety Flow Chart



Appendix 2

Acceptable Use Agreement for Staff

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, email or social networking sites.
Please be aware that this agreement related to both working at school and working remotely.
Use of any school ICT equipment or access to the network implies consent to this Acceptable Use Agreement.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to students before they can upload video or photographs to the internet or send them via email for school work purposes.
- I know that images uploaded by me or my students should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I will report accidental misuse and incidents of deliberate misuse.
- I will report any incidents of concern for a child or young person's safety to the Head teacher, Senior Designated Persons in accordance with the school safeguarding procedures.
- I know who my Designated Safeguarding Leads and Online Safety Lead are.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal email. I know I should only use my school e-mail address to contact a student via their school email address.
- I understand that staff are not permitted to follow or engage with current or prior students of the school on any personal social media network account.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources, onto school computers or online storage areas.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- If I feel I have, or that someone else has been, subjected to abuse by others in a professional capacity through use of a social networking site, then I will report this action using the agreed school safeguarding protocols.

Recorded via Microsoft Forms

Name & Date agreed to

Appendix 3

Acceptable Use Policy for Students

All young people are encouraged to use the computers and mobile technology at Stowmarket High School or when participating in online learning to benefit from the world of opportunities and knowledge that the Internet provides.

However, so that you understand and accept responsibility for keeping yourself and other young people safe when online, it is important that you agree to the following statements.

- I will use the internet to help me learn.
- I will learn how to use the internet safely and responsibly.
- I will only send email messages that are appropriate and will not use group email lists without permission from a member of staff.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- I will not give out passwords or personal information like my full name, address or phone numbers.
- I will not post photographs or video clips of myself, other students or staff without permission and I will not include my full name with photographs or show that I attend Stowmarket High School (e.g. the school badge can be seen on your school uniform).
- If I need help with online safety I know who I can ask.
- If I see anything on the internet that makes me feel uncomfortable, I know what to do e.g. using the CEOP button).
- If I receive a message sent by someone I don't know, I know what to do.
- I know I should follow these guidelines as part of the agreement with my parent/carer.
- I agree to look after myself and others by using my internet in a safe and responsible way.
- I will not publish or distribute personal information about other people from Stowmarket High School such as names, phone numbers or address details, this also includes photographs.
- I will not deliberately damage any hardware, try to bypass the Internet filtering system or install software on the network.
- I will be responsible for my behaviour when using the Internet, this includes resources and websites that I access and the language that I use.
- If I come across any inappropriate or harmful material online, I will report it immediately to a member of staff.
- I understand that my computer use is monitored and recorded and that Internet access is 'filtered'.

- I will not comment or post inappropriately about the school or school staff and understand that any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy.
- I understand that these conditions are designed to keep me safe, and if they are not followed, appropriate sanctions will be applied and my Internet use could be withdrawn.

I will not create, browse, copy, download, forward or post any material:

- *which supports or encourages the use of illegal drugs, substances or criminal activity;*
- *that may be pornographic, racist or illegal;*
- *which might upset people, cause offence or make people feel that they are being bullied; or*
- *that condones violence or intolerance, which would breach copyright or intellectual property laws.*

I may be asked to engage in Online Learning using Microsoft Teams and understand that some lessons may be recorded by teachers. If I do not wish to be recorded I must turn off my camera before I join the lesson.

Student Details – recorded via Microsoft Forms

Name, Tutor Group, Date agreed to

Use of any school ICT equipment or access to the network implies consent to the terms of this Acceptable Use Agreement.

Appendix 4

Organisation/Resource	What it does/provides
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning