St Edmundsbury and Ipswich
Diocesan Multi Academy Trust

St Mary's Church of England Primary School

Online Safety Policy

Adopted: 21st May 2024 Review date: Summer 2025

Ethos statement
The school's Online Safety Policy reflects our Christian vision:
"Love one another. As I have loved you, so you must love one another." John 13:34
Unconditional love underpins all we do at St Mary's Church of England Primary School. We value and embrace the individuality of every child as they discover, learn and flourish in a place of security and love. We are an inclusive school, welcoming all children with respect, understanding and dignity. We have a duty of care to the children and will demonstrate the compassion and understanding that allows all children to flourish. In the context of this policy, this means that we aim to provide a safe and welcoming environment, in which children can learn, underpinned by a culture of openness where both children and adults feel secure, are able to raise concerns and believe they are being listened to, and that appropriate action will be taken to keep them safe. We recognise the moral and statutory responsibility placed on all staff to safeguard and promote the welfare of all children.

Introduction
The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation and technology often provides the platform that facilitates such harm.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The school adopts a whole school approach to online safety to protect and educate pupils and staff in their use of technology, and establishes mechanisms to identify, intervene in, and escalate any concerns as appropriate.

The Local Governing Body recognises the need to ensure that it complies with its duties under legislation and this policy has regard to statutory guidance, Keeping Children Safe in Education (KCSiE), Working Together to Safeguard Children and locally agreed inter-agency procedures put in place by Suffolk Safeguarding Partnership Board.

This policy will be reviewed annually, as a minimum, and will be made available publicly via the school website or on request.

Safeguarding and promoting the welfare of children is defined as: protecting children from maltreatment; preventing impairment of children's mental and physical health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes.

This policy is for all staff, parents, governors, volunteers, supply staff, contractors and the wider school community. It forms part of the child protection and safeguarding arrangements for our school and is one of a suite of policies and procedures which encompass the safeguarding responsibilities of the school. In particular, this policy should be read in conjunction with the school's Child Protection and Safeguarding Policy, Code of Conduct (including Acceptable Use of ICT), Safer Recruitment Policy, Behaviour Policy and Anti-Bullying Policy, Child-on-Child Abuse Policy and procedures, and Part One of Keeping Children Safe in Education, copies of which will be provided to all staff on induction. This policy should also be read in conjunction with Part Two of Keeping Children Safe in Education, particularly the sections on opportunities for teaching safeguarding and online safety, and the separate DfE guidance Teaching Online Safety in Schools (2023).

Aims

This policy aims to explain how staff members, parents/carers or children can be a part of these safeguarding procedures. It also details how children 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 children, young people and adults from potential and known risks.

- To emphasise the need to educate staff, children and young people 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 pupil, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Roles and Responsibilities of the School

It is the responsibility of all staff members to know who the Designated Safeguarding Lead Person is and to record and report any safeguarding concerns relating to online safety according to the school's safeguarding procedures (see Child Protection and Safeguarding Policy).

Governors and Designated Safeguarding Lead

At St Mary's CE Primary School, the Designated Safeguarding Lead (DSL) is the Headteacher (see Safeguarding Policy). It is the overall responsibility of the DSL with the Governors to ensure that there is an overview of online safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The DSL is designated as the Online Safety Lead, to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who takes this role within the school.
- The DSL and the Governing Body ensure that there is a disclaimer on e-mails stating that the views expressed are not necessarily those of the school or the MAT (on the main school email address).

- Time and resources should be provided for the Online Safety Lead and staff to be trained and update policies, where appropriate.
- The DSL is responsible for promoting online safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The DSL should keep Governors informed of online safety developments and ensure Governors understand the link to safeguarding.
- The Governors **MUST** ensure online safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded. There is a checklist for this purpose in Appendix 4 of this policy.
- An Online Safety Governor (at St Mary's School, this is the Safeguarding Governor) challenges the school about appropriate procedures, the management and teaching of online safety.

  The Online Safety Governor will challenge the school about:

  - Filtering and monitoring systems;
  - Online safety as a running and interrelated theme in relevant safeguarding policies;
  - Having policies and procedures about the acceptable use of personal devices;
  - How online safety is included in the planned curriculum;
  - Ensuring that any misuse of technology or concern about a child's safety has been dealt with appropriately, according to policy and procedures and appropriate action is taken.

Local Online Safety Lead (DSL) and ICT / Computing Subject Leader

It is the role of the DSL, alongside the Computing subject leader, to:

- Appreciate the importance of online safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Raise awareness and maintain a safe ICT learning environment within the school e.g. by displaying online safety posters and sending home leaflets.
- Keep parents informed of online safety issues e.g. by organising workshops / adult learning opportunities and sending home leaflets.
- Ensure that the Acceptable Use Policy is reviewed annually, with up-to-date information and that staff members and parents feel informed and know where to go for advice.
- Ensure that filtering and monitoring systems are sufficient and up-to-date and that filtering is set to the correct level for staff, children and young people.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Ensure staff are familiar with changing technologies and how they are used and accessed, including use of apps, tablets and other 'smart' devices, including wearable technologies.
- Report serious concerns to the Governing Body. Technical issues are reported to the Standards Committee and the Finance Committee if there are cost implications. Safeguarding concerns, which may include online safety issues, are reported to the Personnel Committee and the Local Governing Body via the termly Headteacher's Report.

- Liaise with the PSHE and Computing leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Remind staff about the Acceptable Use Policy and monitor whether it is being adhered to. Any minor irregularities, such as unauthorised software, will be reported to the member of staff to rectify. Serious breaches will be reported to the Governors.
- Record safeguarding incidents or risks (see Child Protection and Safeguarding Policy).
- Alert staff to the issue of viruses being transmitted via new programmes and memory sticks and remind them to take care when transferring data.
- Ensure that staff are aware that if they use a memory stick, it must be one supplied by the school and encrypted because of the risk of viruses and data security.
- Remind staff to beware of unsolicited e-mails from other sources. Any concerning emails must be reported to the school's ICT technical support staff.

Staff or Adults

It is the responsibility of all adults within the school to:

- Be familiar with the Child Protection and Safeguarding, Whistleblowing, Behaviour, Anti-Bullying 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 DSL immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Be familiar with and adhere to the Acceptable Use Policy.
- Report any safeguarding concerns to the DSL, following the procedures in the Child Protection and Safeguarding Policy, including recording the concern on CPOMS (the school's online safeguarding recording system).
- Report technical concerns e.g. about filtering to the Computing Subject Leader / ICT Technician.
- Report accidental access to inappropriate materials to the DSL / Computing Subject Leader / ICT Technician in order that inappropriate sites are added to the restricted list or access can be controlled. (The DSL / Computing lead would, in turn, report to the ICT Technician to resolve the issue.)
- Alert the DSL of any new or arising issues and risks that may need to be included within policies and procedures.
- Raise children's awareness of online safety so that they can use technology in a safe way. Children 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.
- Be familiar with changing technologies and how they are used and accessed, including use of apps, tablets and other 'smart' devices.
- Report incidents of personally directed 'bullying' or other inappropriate behaviour via the Internet or other technologies using the behaviour reporting procedure in the same way as for other non-physical assaults. At St Mary's, staff record behaviour incidents, including online safety issues on CPOMS, the schools online recording system.

- Check searches and websites prior to lessons so that the chance of children seeing inappropriate material is minimised.

Online Safety Risks

Online safety issues can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful content, for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, or radicalisation or extremism;
- **Contact**: being exposed to harmful online interaction with other users, for example, peer to peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and online bullying); and
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If staff feel that either they or pupils are at risk this should be reported to the Anti-Phishing Working Group (https://apwg.org/).

It is important for staff members and governors to be aware of the 4Cs (above) and to consider them when devising policies, monitoring and evaluating practice and planning the teaching of online safety at an age-appropriate level. For example, pupils will be taught about respectful online conduct and the impact of online bullying.

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in. There are separate networks and passwords for staff members and visitors.

All staff should be familiar with the school's Code of Conduct and Acceptable Use Policy and the Acceptable Use Agreement (Appendix 5), which they need to sign and return to the DSL to kept on file.

Concerns about the conduct of adults should be pursued in line with the Children Protection and Safeguarding Policy and Whistleblowing Policy.

Children

Children should be:

- Responsible for following the Acceptable Use Policy for Older Pupils (Appendix 2) whilst within St Mary's CE Primary School as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.
- Taught to use the internet in a safe and responsible manner through Computing, PSHE or other clubs and groups.
- Responsible for following instructions and rules that are designed to keep them safe when using technology. Children in Key Stage 2 are asked to sign an Acceptable Use Policy for Children (Appendix 2) as part of the school's efforts to raise awareness.

- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

In the Event of Inappropriate Use by Children

The Acceptable Use Policy for Children (Appendix 2) details how children are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people 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 polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

St Mary's C of E Primary School encourages parents/carers to support the agreement with their child. This is also intended to provide support and information to parents/carers when children and young people 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 technology in or beyond school.

Should a child be found to misuse the online facilities whilst at school, the following consequences should occur.

- Any child found to be misusing the internet by not following the Acceptable Use Policy for Children may be suspended from using the internet for a particular lesson or activity.
- Further misuse of the agreement may result in not being allowed to access the internet for a period of time and parents/carers may be informed.
- Parents/carers may be contacted to raise awareness where a child or young person is deemed to have misused technology against another child or adult.

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 feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.

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.

Pupils' misuse of the internet or technology in school is considered a behaviour or safeguarding issue (depending on the nature of the incident) and is dealt with according to the relevant policies.

The Curriculum and Learning

Internet Use

The school's computing curriculum (Teach Computing) includes opportunities for the children to learn about online safety through specific online safety lessons. Teaching is age and developmentally appropriate. The curriculum content covers:

- **Evaluating** what they see online, including judging whether what they see is true, valid or acceptable.
- **Recognising techniques used for persuasion**, including how people/companies persuade people to buy something or believe that something false is true.
- **Online behaviour**, including applying the same standards as for offline behaviour and recognising unacceptable online behaviour from others.
- **Identifying online risks**, including ways someone might put themselves at risk online, online reputation and the risks of cyber-crime, online fraud and identity theft.
- **How and when to seek support.**

Online safety is also covered through the school's PSHE curriculum (based on PSHE Association plans) and lessons on keeping safe.

Through strong promotion of the school's Christian vision and values and regularly giving children opportunities to share their perceptions, we foster a culture in which children know who to turn to if they need help or if they do not feel safe. Children are encouraged to share their concerns with adults in school, particularly their class teacher and Pastoral Support staff. The school's PSHE curriculum emphasises children's wellbeing and safety through relevant PSHE lessons, themed 'safety' days and appropriate visitors, such as the PCSO and school nursing team. Where appropriate, it is daily practice for children to be taught explicitly about keeping safe in other lessons, such as computing, swimming, PE and Design Technology.

Keeping safe online includes being aware of the need to keep personal data secure and 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 another establishment.
- Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school.
- Identifying information, e.g. I am number 8 in the school Football Team.

Other aspects of harm and risk that must be covered include:

- Age restrictions
- Privacy settings
- Fake website and online / email scams
- Password phishing
- Identifying abusive behaviour
- Radicalisation
- Impact on quality of life, physical and mental health and relationships.

Children should be supervised and monitored when they have access to the internet during school time. The management of internet use and the risks associated with this should be considered by teachers when planning lessons. Pupils' misuse of the internet or technology in school is considered a behaviour or safeguarding issue (depending on the nature of the incident) and is dealt with according to the relevant policies.

Pupils with Additional Learning Needs

The school should 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 pupil 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, acknowledging that the pupil may be particularly vulnerable. Staff members must be aware that extra vigilance may be required and must monitor the pupil's learning more frequently and robustly.

School Website and Social Media

When children join St Mary's, the school seeks the permission of parents for photographs to be taken of children and for those images to be used for a range of purposes, including on the school website and Facebook page. Photographs are not published alongside the names of children. The Headteacher, Chair of Governors, teachers, administrative staff and the ICT Technician have passwords for accessing and editing pages on the website, for example for subject leaders to update subject-specific information online. A small group of staff members volunteer to post information and news about the school on social media, such as the school's Facebook page. They maintain social media pages and keep usernames and passwords private, so that only school staff can act as administrators. Parents do not act as administrators on the school website or social media accounts except in special circumstances at the discretion of the Headteacher.

External Websites

In the event that a member of staff or child finds themselves or another person on an external website e.g. as a victim of cyber-bullying, he / she is encouraged to report this to the DSL and any other appropriate authority depending upon the nature of the incident. This incident must then be recorded on CPOMS, the school's online recording system, and addressed using the school's usual safeguarding and behaviour procedures.

E-mail Use

The school may have e-mail addresses for children to use, as a class and or as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms. Email may be used to correspond with children from other schools or countries and can be used to enhance the curriculum in many ways. Teachers are expected to monitor class use of emails where there are communications during school time.

Children should use school issued email addresses for approved communication only e.g. with a 'pen pal' from a partner school. A breach of this may be considered a misuse.

Parents/carers are encouraged to be involved with the monitoring of emails sent from home, understanding who their child is communicating with and for what purpose, assessing risks together.

Mobile Phones, Smart Devices & Other Emerging Technologies

Increasing numbers of children have access to mobile phones and other 'smart' technologies and may bring them to school.

Pupils may bring mobile phones to school. However, it is expected that pupils' mobile phones are handed in to a member of staff at the start of the day. Pupils' mobile phones are kept securely in the main office and should be collected by pupils at the end of the day. Pupils must not use mobile phones during the school day. Pupils are discouraged from wearing smart watches and other wearable technology in school because of the risk of expensive items being lost, broken or stolen. However, pupils may wear smart watches at their own risk. The school accepts no responsibility for the loss, damage of theft of mobile devices or wearable technology.

Pupils must not use any smart or wearable technology during tests or examinations.

The use of mobile technologies can be used as a teaching and learning tool within the curriculum. In particular, teachers are expected to deliver age-appropriate learning about the safe use of mobile devices and the internet in PSHE and computing. The following areas of concern are addressed by the strict control of the use of technology in school and may be covered at an age-appropriate level in PSHE and computing. If such issues occur outside school then, they will be addressed in line with relevant policies, such as the policies for Behaviour and Anti-Bullying.

- Inappropriate or bullying text messages.
- Images or video taken of adults or peers without permission being sought.
- 'Happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed.
- 'Trolling' – the defaming of another person's character through persistent dialogue, gossip, spreading rumours or inciting argument
- 'Sexting' - 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.
- The safeguarding risks relating to contact between children and staff members using smart technologies.

Personal Mobile Devices

Staff are allowed personal mobile phones or devices for their own use, subject to the restrictions in the Acceptable Use Policy and Code of Conduct.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business. School phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in the Acceptable Use Policy.

Users should take note of the following guidance from the school's Code of Conduct:

As with all personal possessions, the school is not responsible for the security of personal devices. Staff members must be sensitive about their roles in school and personal devices, including mobile phones, should only be used at appropriate times.

- Phones should be silent during lesson times.
- Employees should not make or receive calls in front of pupils or during lesson times or during times when they are expected to be working (i.e. not break times).
- Phones should not be used to record and keep images or footage of pupils.

It is recognised that imposing rigid regulations or 'bans' can be counterproductive and can lead to a culture of secrecy, suspicion and uncertainty. Therefore, this code operates on a basis of professional trust with regard to the use of personal mobile phones. There may be times when exceptional personal circumstances require more flexibility. This should be negotiated with a Senior Leader or the Headteacher.

Staff must ensure that there is no inappropriate or illegal content stored on personal devices brought into school and should be aware that using features, such as video or sound recording, are subject to the same procedures as taking images from digital or video cameras.

Staff should be aware that games consoles such as the Sony PlayStation, Microsoft Xbox and other such systems have Internet access which may not include filtering. Before use within school/education setting or other establishment, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.

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.

When in school, children have access to a variety of visual and sound recording equipment.

The sharing of photographs via weblogs, social media 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 a 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 a school website. Photographs should not be presented alongside a child's name for safeguarding reasons.

It is current practice by some external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children will only be used after permission has been given by a parent/carer.

Managing Social Networking - Pupils

Social networking sites, such as Facebook, Instagram and WhatsApp, have emerged in recent years as a leading method of communication, proving increasingly 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 are in place:

- Social networking sites should not be accessed during the school day – pupils should not have access to personal mobile devices in school and school equipment must only be used for the purposes set out by staff members in lessons.
- Children are advised against giving out personal details or information.
- Pupils are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse.
- 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.
- Staff members are aware that social networking can be a vehicle for cyber-bullying and pupils are taught explicitly about online conduct. 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.
- Pupils and parents are reminded of relevant age restrictions as appropriate.

Social Networking Advice for Staff

Social networking outside of work hours, on non-school equipment, is the personal choice of all school staff. However, 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 or parents, 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 pupils or parents 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 pupils outside of Headteacher authorised systems (e.g. school email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent pupils or parents from accessing photo albums or personal information.

See the Acceptable Use Policy and Code of Conduct for more information about acceptable and unacceptable online conduct. Further advice about social networking can be found in Appendix 6.

Review

The governing body will ensure that an annual review is undertaken of the school's approach to online safety including the school's filtering and monitoring provision, supported by an

annual risk assessment that considers and reflects the risks pupils face online. The review should include a member of the senior leadership team, the DSL, the IT service provider and a governor.

Filtering and Monitoring

The school ensures they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on cyber security including considerations can be found at Cyber security training for school staff - NCSC.GOV.UK

The school uses Smoothwall Monitor filtering and monitoring software, managed by the school's IT Technician in conjunction with the Online Safety Lead.

At St Mary's the Online Safety Lead is the Designated Safeguarding Lead. The DSL ensures that information and reports regarding filtering and monitoring are shared with the Named Governor for Safeguarding. Systems for filtering and monitoring are included in an annual review of online safety.

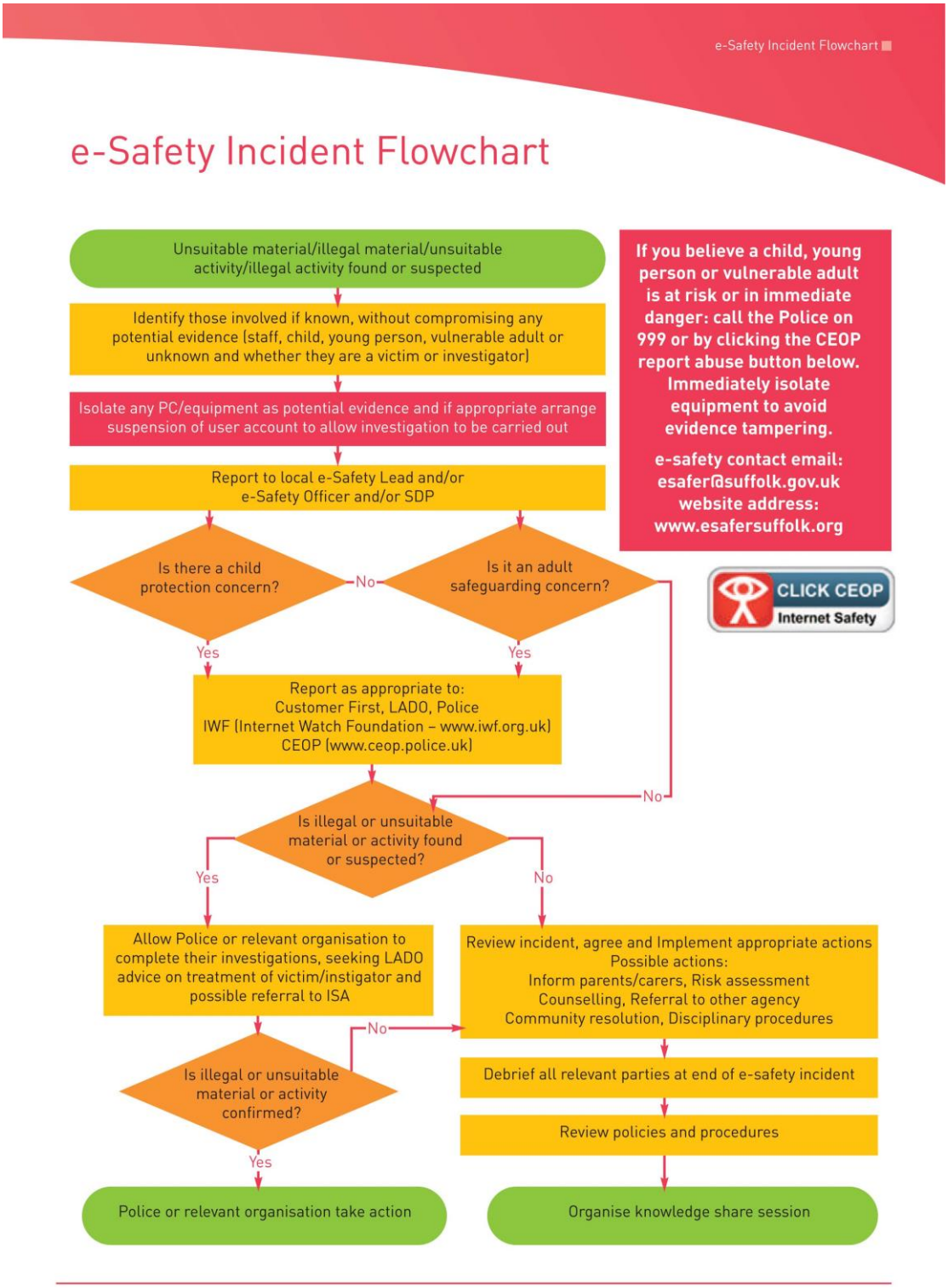
Links to Other Policies - Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or social networks. The school has an Anti-bullying Policy, which refers to cyber-bullying issues.

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 computing and PSHE materials for children 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 Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour.

Allegations of misuse against members of staff should be dealt with according to the school's Child Protection and Safeguarding Policy. This may involve referring an incident to the Local Authority designated Officer (LADO) without internal investigation.

Appendix 1
Online Safety Flow Chart



Appendix 2: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4

Online Safety Checklist

Policies, practice and monitoring	Yes	No	Action
Does the school have an Online Safety Policy and an Online Safety Lead in place?			
Are there 'Acceptable Use Policies' for both pupils and adults?			
Is cyber bullying addressed in the school's Anti-Bullying policy?			
Does the school keep a log of online safety incidents and alter provision accordingly?			
Infrastructure	**Yes**	**No**	**Action**
Is the school network safe and secure? *E.g. through filtering / monitoring.*			
Does the school respond if pupils report accessing inappropriate content?			
Learners	**Yes**	**No**	**Action**
Do learners understand what safe and responsible online behaviour means and do they use it?			
Is online safety education a regular part of the curriculum?			
Do learners know how to report online safety concerns? *E.g. CEOP Report Abuse button, reporting to an adult in school*			
Staff	**Yes**	**No**	**Action**
Do staff understand online safety issues and risks? *E.g. through training / updates*			
Do staff know who to report to with an issue of concern regarding online safety?			
Do staff keep data safe and secure? *E.g. assessment data, use of passwords*			
Do staff take measures to protect themselves online? *E.g. keep personal information private, use secure passwords*			
Do staff conduct themselves professionally online? *E.g. social networking sites*			
Parents / Governors	**Yes**	**No**	**Action**
Do governors understand online safety issues and risks?			
Does the school keep parents aware of e-safety issues, e.g. through newsletters, leaflets, open assemblies, updates etc?			

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police