



# Online Safety and Acceptable Use Policy

**Policy updated: September 2024**  
**To be reviewed by: September 2025**

Reviewed by: Katie Hammond; LGB

## Version Control

Date	Change
<b>July 2018</b>	Policy updated and written in line with online safety curriculum (Educated for a connected world)
<b>Sept 2020</b>	Minor amendments made
<b>Sept 2022</b>	New vision statement added, minor amendments including links to old policies taken off.
<b>Nov 2022</b>	Parents and carers and Staff responsibility updated to include recent KCSiE 22 updates. Minor amendments made to links, remote learning and aims.
<b>Sept 2023</b>	Appendices changed to reflect current Online Safety Agreement. Minor amendments to Online Safety Leader's name and inclusion of Google Classroom as an educational tool. Information on Smoothwall filtering and IMPERO monitoring added. Sections reordered for clarity; minor amendments and reformatting.
<b>Sept 2024</b>	Minor amendments to keep up to date with KCSiE 2024

## Contents

<b>1. Aims</b> .....	4
<b>2. Legislation and Guidance</b> .....	5
<b>3. Roles and Responsibilities of the School</b> .....	5
3.1 Headteacher and Governing Body.....	5
3.2 Role of the Online Safety Governor.....	6
3.3 Online Safety Lead .....	6
3.4 The ICT Technician .....	7
3.5 All Staff and Volunteers .....	7
3.6 Pupils .....	8
3.7 Parents.....	8
<b>4. Appropriate and Inappropriate Use</b> .....	8
4.1 Key Documents.....	8
4.2 Procedure in the Event of Inappropriate Use by Teaching and Support Staff .....	9
4.3 Procedure in the Event of Inappropriate Use by Pupils .....	9
<b>5. Cyber-Bullying</b> .....	9
5.1 Definition .....	9
5.2 Preventing and Addressing Cyber-Bullying.....	9
<b>6. Use of Technology</b> .....	10
6.1 Digital and Video Images .....	10
6.2 Mobile Phones and Other Emerging Technologies .....	10
6.3 Examining Electronic Devices .....	10
6.4 Personal Mobile Devices .....	11
6.5 School-Issued Mobile Devices .....	11
6.6 Video and Webcams.....	11
6.7 How the School will respond to Issues of Misuse .....	11
<b>7. Safeguarding Measures: Filtering and Monitoring</b> .....	12
<b>8. Training and Education</b> .....	12
8.1 Staff Training.....	12
8.2 Educating Pupils about Online Safety.....	13
8.3 Educating Parents about Online Safety and Additional Support.....	14
<b>9. Links to Other Documents and Policies</b> .....	14
<b>Appendix 1: Online Safety Training Needs – Self Audit for Staff</b> .....	16
<b>Appendix 2: E-Safety Incident Flowchart</b> .....	17
<b>Appendix 3: Acceptable Use Agreement for Staff, Governors and Visitors</b> .....	18
<b>Appendix 4: ICT Class Agreement</b> .....	19
<b>Appendix 5: Pupil and Parents’ Online Safety Agreement</b> .....	20
KS1 Internet Rules .....	20
KS2 SMART Online Safety Rules .....	22

**At All Saints' we are 'Children of God'.  
We wear our crowns with pride.  
Together, we are Included, Involved and Inspired.**

- 24 Do you not know that in a race all the runners run, but only one gets the prize?  
Run in such a way as to get the prize.
- 25 Everyone who competes in the games goes into strict training. They do it to get a  
crown that will not last; but we do it to get a crown that will last forever.
- 26 So I run with purpose in every step.

*1 Corinthians 9: 24-26*

**Vision Statement**

*At All Saints' everyone is welcomed and **included**. Each individual is acknowledged and valued as an equal member of our school family and we form a community where we worship God together freely. We celebrate our inclusivity and are respectful of our differences.*

*Our emblem is a crown; we wear it with pride because it reminds us that we are working for a purpose. This means that we are **involved** in our learning and are determined to take whatever action is needed for us to be the best that we can be.*

*We seek a clearer understanding of the world and confidently imagine a better future. With our eyes fixed on this prize, we are **inspired** to be life-long learners and we want to inspire others too to make a difference in this world.*

***Together · Included · Involved · Inspired***



**St Edmundsbury and Ipswich**  
Diocesan Multi Academy Trust

## 1. Aims

New online technologies have become integral to the lives of children and adults in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. They stimulate discussion, promote creativity and increase awareness of context to promote effective learning. It is the duty of the School to ensure that pupils are protected from potential harm both within and beyond the environment.

This policy aims to explain how parents/carers, and pupils can be a part of these protecting/safeguarding procedures. It applies to all members of the school community (including Staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both inside and out of school.

It details how pupils are educated to be safe and responsible users, capable of making good judgements about what they see, find and use through technology. The term 'online safety' is used to encompass the safe use of all technologies in order to protect pupils and adults from potential and known risks by:

- establishing clear mechanisms to identify, intervene and escalate an incident, where appropriate
- providing robust safeguards and agreement for acceptable use to guide all users, whether Staff or pupil, in their online experiences
- delivering an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- ensuring adults are clear about procedures for misuse of any technologies both within and beyond the School
- developing 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

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

- access to illegal, harmful or inappropriate images or other content
- unauthorised access to/loss of/sharing of personal information
- sharing/distribution of personal images without an individual's consent or knowledge
- inappropriate communication/contact with others, including strangers
- online bullying
- access to unsuitable video/internet games
- an inability to evaluate the quality/accuracy and relevance of information on the internet
- plagiarism and copyright infringement
- illegal downloading of music or video files
- the potential for excessive use which may impact on the social and emotional development and learning of the pupil
- cyber addiction and/or validation through social media

Many of these risks reflect situations in the off-line world and it is essential that this **Online Safety and Acceptable Use Policy** is used in conjunction with other school policies (e.g. **Behaviour Policy**, **Child Protection and Safeguarding Policy** and **Mobile Phone Policy**).

It is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build pupils' knowledge and resilience, and understanding of the risks they may face, as well as how they can keep themselves safe.

## 2. Legislation and Guidance

This policy is based on the Department for Education (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education \(KCSiE\)](#) and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Education for a connected world framework](#)
- [Searching, screening and confiscation](#)
- [Using external expertise to support online safety](#)

It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

## 3. Roles and Responsibilities of the School

### 3.1 Headteacher and Governing Body

It is the overall responsibility of the Headteacher 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 Headteacher has designated Anna O'Hare as the Online Safety Lead. Her role is to implement agreed policies, procedures, staff training, curriculum requirements and to take responsibility for ensuring online safety is addressed in order to establish a safe ICT learning environment. All Staff and pupils are aware of who has this role within the School.
- Time and resources should be provided for the Online Safety Lead and all other Staff to be trained and update policies, where appropriate.
- The Headteacher and Online Safety Lead are responsible for promoting Online Safety across the curriculum. They are aware of how Online Safety is being developed in the School through the School Development Plan.
- The Local Governing Body will co-ordinate regular meetings with appropriate Staff to discuss Online Safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).
- The Governors MUST ensure that Safeguarding procedures cover Online Safety is recognised as a key area of Safeguarding and know how it is being addressed within the School. It is the responsibility of Governors to ensure that all Safeguarding guidance and practices are embedded.
- Governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an

awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. (see *KCSiE 2024*, paragraph 140, p. 39)

- Governors will ensure that they have read and understood this policy
- Governors will agree and adhere to the terms on Acceptable Use of the School's ICT systems and the internet.

This list is not intended to be exhaustive.

### 3.2 Role of the Online Safety Governor

A member of the governing body will take on the role of the Online Safety Governor. The role of the Online Safety Governor includes regular meeting with the Online Safety Lead and with the School's Designated Safeguarding Lead to discuss current issues and monitor online incidents. The Online Safety Governor will challenge the School to ensure that:

- the School has in place:
  - an **Acceptable Use Policy** (AUP)
  - an **Online Safety Agreement** (Appendix 4)
  - firewalls.
  - anti-virus and anti-spyware software.
  - filters.
  - an accredited ISP (internet Service Provider).
  - awareness of wireless technology issues.
  - a clear policy on use of personal devices.
  - a clear policy on use of social media platforms
- any misuse or incident has been dealt with appropriately, according to policy and procedures (see the **Managing Allegations Procedure** on Suffolk Local Safeguarding Children's Board website), and appropriate action is taken, even to the extreme of suspending a member of staff, informing the Police (via establishment's agreed protocols with the Police) or involving parents/carers.

This list is not intended to be exhaustive.

### 3.3 Online Safety Lead

It is the role of the designated Online Safety Lead to:

- take day-to-day (agreed by the School's DSL) responsibility for online issues and have a leading role in establishing and reviewing the School's **Online Safety Policy**.
- produce weekly reports using the IMPERO monitoring system to review improper use.
- ensure that the **Online Safety and Acceptable Use Policy** and **Online Safety Agreement** are reviewed annually with up-to-date information, and that training is available for all Staff to teach Online Safety, and for parents to feel informed and know where to go for advice.
- ensure that all adults are aware of the filtering levels and reports (IMPERO and Smoothwall) and why they are there to protect pupils, and to suggest training where available.
- liaise with the PSHE, Safeguarding and ICT leads so that policies and procedures are up-to-date and take account of any emerging issues and technologies.
- update staff training (for all Staff) in response to new and emerging technologies so that the correct Online Safety information can be taught or adhered to. (Appendix 1 contains a self-audit for Staff on online safety training needs)
- lead training to support the use of *ClassDojo*, *Seesaw*, *Google Classroom*, *Tapestry* and any other online apps used.



- monitor the use of the Internet and online technologies as well as social media platforms created by and used for school, including *Facebook, Instagram, ClassDojo, Google Classroom* and *Tapestry*
- ensure any incidents of cyber bullying, child-on-child abuse, and online safety are logged and dealt with appropriately on CPOMS, in line with this policy and the **Behaviour Policy**
- work alongside the ICT technician to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone PCs, teacher laptops and pupil laptops, and that this is reviewed and updated on a regular basis
- liaise with other agencies and/or external services if necessary.

This list is not intended to be exhaustive.

### 3.4 The ICT Technician

The ICT Technician is responsible for:

- putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ensuring that the School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- conducting a full security check and monitoring the School's ICT systems on a half-termly basis
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy

This list is not intended to be exhaustive

### 3.5 All Staff and Volunteers

It is the responsibility of all adults within the School to ensure that they:

- maintain an understanding of this policy and implement it consistently.
- work with the DSL/Online Safety Lead to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- are familiar with the **Behaviour Policy, Anti-Bullying Policy, Child Protection and Safeguarding Policy** 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 Headteacher/DSL immediately, who should then follow the **Managing Allegations Procedure** where appropriate.
- 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 pupils are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Pupils should know what to do in the event of an incident.
- have an up-to-date awareness of online safety matters and of the current school policy and practices
- agree and adhere to the terms on Acceptable Use to show that they accept the agreement for Staff using non-personal equipment within and beyond the school environment (Appendix 3), unless otherwise instructed or agreed.

- use electronic communications in an appropriate way that does not breach the [Data Protection Act](#)
- ensure that any incidents of cyber-bullying (child-on-child abuse) are dealt with appropriately in line with our **Behaviour Policy**.

This list is not intended to be exhaustive.

### 3.6 Pupils

Pupils are responsible for using school IT systems in accordance with the School's **Online Safety Agreement** (Appendix 5) and **ICT Class Agreement** (Appendix 4), which they will be expected to read and sign before being given access to school systems. They will:

- take responsibility for following the **Acceptable Use Agreement** whilst within school as agreed at the beginning of each academic year or whenever a new pupil attends the school for the first time.
- be taught to use the internet in a safe and responsible manner through ICT, PSHE (LIFE) teaching or other clubs and groups.
- be 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).
- understand the importance of accepting good online practices when using digital technologies outside of school, including during remote learning, and realise the **Online Safety Agreement** also covers their actions out of school, if related to their membership of school.

### 3.7 Parents

Parents are expected to:

- notify a member of staff or the headteacher of any concerns or queries regarding this policy
- ensure that they and their child have read, understood and agreed to the terms of the **Online Safety Agreement**, sent home to parents in September 2023 (Appendix 4)
- in the event of remote learning, parents should encourage daily engagement and completion of tasks (where possible) using either *ClassDojo* (KS1/KS2) or *Tapestry* (EYFS)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)
- Parent guides for social media platforms – [parent zone](#)

## 4. Appropriate and Inappropriate Use

### 4.1 Key Documents

All Staff should receive a copy of the **Online Safety and Acceptable Use Policy** and a copy of the **Acceptable Use Agreement**, which they need to sign and return to school, to be kept on file.

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. *Please refer to Appendix 3 for the complete Acceptable Agreement for Staff.*



## 4.2 Procedure in the Event of Inappropriate Use by Teaching and Support Staff

It is expected that all members of the School will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or – very rarely – through deliberate misuse.

If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report must be made to the Headteacher/DSL immediately and then the **Managing Allegations Procedure** and the **Child Protection and Safeguarding Policy** must be followed to deal with any misconduct and all appropriate authorities contacted.

## 4.3 Procedure in the Event of Inappropriate Use by Pupils

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

- parents of any pupil found to be misusing the internet, by not following the **Acceptable Use Agreement**, will receive a letter or phone call, explaining the reason why the pupil's use has been suspended for a particular lesson or activity.
- Misuse of the agreement may result in not being allowed to access the internet for a period of time and parents/carers will receive another letter or phone call. This will also be logged on CPOMS.

In the event that a pupil **accidentally** accesses inappropriate materials, they should report this to an adult immediately.

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

# 5. Cyber-Bullying

## 5.1 Definition

Cyber-bullying takes place online, for example, through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (see also the school **Behaviour Policy**)

## 5.2 Preventing and Addressing Cyber-Bullying

To help prevent Cyber-Bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including situations where they are a witness rather than the victim.

The School will actively discuss Cyber-Bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss Cyber-Bullying with their class, and the issue will be addressed in assemblies.

Teaching Staff are also encouraged to find opportunities to use aspects of the curriculum to cover Cyber-Bullying. This includes Personal, Social, Health and Economic (PSHE) education, and other subjects where appropriate.

All Staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of Safeguarding training (see Section 16 for more detail on training).

In relation to a specific incident of cyber-bullying, the School will follow the procedures set out in the school **Behaviour Policy**. Where illegal, inappropriate or harmful material has

been spread among pupils, the School will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the Police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the **MAT Complaints Procedure**.

## 6. Use of Technology

### 6.1 Digital and Video Images

Photographs should only be uploaded on the approval of a member of staff and parent/carer and should only contain something that would also be acceptable in 'real life'. Images of pupils should be stored according to policy.

*Any photographs or video clips uploaded should not have a file name of a pupil, especially where these may be uploaded to the school website. Safeguarding guidance states either a pupil's name or a photograph may be used, but not both together.*

Staff are allowed to take digital/video images to support educational aims, but must follow school policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of Staff should not be used for such purposes unless permission is given by a member of SLT.

Students' name/photographs will not be used online without a signed consent form from their parent/carer. Permission is requested on admission to the School.

### 6.2 Mobile Phones and Other Emerging Technologies

All Saints' School has made the decision that pupils should have no access to mobile phones on school premises during school hours. Any use of mobile devices in school by pupils must be agreed by the Class Teacher and/or the SLT.

Any breach of the **Acceptable Use Agreement** by a pupil may trigger disciplinary action in line with the school **Behaviour Policy**, which may result in the confiscation of their device.

Mobile phones/tablets may be used by pupils for remote online learning in the event of school closure.

### 6.3 Examining Electronic Devices

School Staff have the specific power under the **Education and Inspections Act 2006**, and increased by the **Education Act 2011** to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, Staff must reasonably suspect that the data or file in question has been, or could be, used to:

- cause harm, and/or
- disrupt teaching, and/or
- break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- delete that material, or
- retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- report it to the Police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

#### 6.4 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 pupils**.

Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that use of features such as video or sound recording may be subject to the same procedures as taking images with digital or video cameras.

Staff should be aware that games consoles such as the Sony play station, Microsoft Xbox, Nintendo Wii and DSi and other such systems have internet access which may not include filtering. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.

Personal mobile phones may be used by Staff to contact parents during school time or on a school trip or residential but Staff should remove their caller ID.

#### 6.5 School-Issued Mobile Devices

The management of the use of these devices should be similar to those stated above, but with the following additions:

- staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the School's terms of Acceptable Use, as set out in Appendix 3.
- staff members must ensure that their work device is secure and password-protected, and that they do not share this password with pupils. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the School should be encrypted.
- if Staff have any concerns over the security of their device, they must seek advice from the ICT Technician.

#### 6.6 Video 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 the School. This process should always be supervised by a member of staff and a record of dates, times and participants held by the School. Pupils need to tell an adult immediately of any inappropriate use by another pupil or adult (this is part of the **Acceptable Use Agreement**).

Where video conferencing is used in the event of remote learning, there must be two members of staff present to ensure accountability.

#### 6.7 How the School will respond to Issues of Misuse

Where a pupil misuses the School's ICT systems or the internet, we will follow the procedures set out in our policies on internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device, where the action constitutes misconduct, the matter will be dealt with in accordance with the **MAT Disciplinary Procedure/Staff Code of Conduct**. The action

taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The School will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the Police.

## 7. Safeguarding Measures: Filtering and Monitoring

The Smoothwall broadband connectivity has a filter system which is set at an age-appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the pupil. All internet access in school is via a proxy server; this is set at 8080 for pupils and 9000 for adults. The pupils' level places stringent controls on what can be accessed on the internet and also does not allow the pupil to import or export documents/programs etc. from any external media (usb drive/cd/external hard drive). Our SCC broadband connection has a firewall and filter that allows us to run basic reports. We review our monitoring and filtering every 6 months to keep it up to date and appropriate.

All Saints' buys into the County Broadband service (Smoothwall); we employ an ICT Technician who ensures that these filters/proxy settings are all set-up correctly and reports and manages any required alterations. Sophos anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.

The School uses Impero to monitor any incidents that need to be followed up for safeguarding purposes. 'Captures' are when a possible issue is flagged up by a 'check' against IMPERO's rules. IMPERO is used during lessons to monitor pupil access and see any captures in real-time. IMPERO reports are run on a weekly basis by the ICT lead to show any historic captures.

We counter 'overblocking' by reporting blocked sites to the IT technician or the ICT Helpdesk for them to unblock.

A firewall ensures information about pupils and the school cannot be accessed by unauthorised users.

The 'Report Abuse' button is available should there be a concern of inappropriate or malicious contact made by someone unknown. However, the pupils know that in the first instance, they should tell the member of staff present, and they will take note or screen shot the offending page and then report the matter to the ICT Technician. *It should be noted that to-date, with all the filters/proxys/firewall in place, we have had no case of inappropriate or malicious contact.*

Students and Staff are forbidden to use any technology designed to circumvent, avoid or bypass any school 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. Please refer to Section 5.

## 8. Training and Education

### 8.1 Staff Training

**All Staff members** will receive:

- training on safe internet use and online Safeguarding issues, including Cyber-Bullying and the risks of online radicalisation as part of their induction when they join the School
- refresher training at least once each academic year as part of Safeguarding training, as well as relevant updates as required (for example, through emails, discussions and staff meetings)

- training on *ClassDojo*, *Seesaw*, *Google Classroom* and/or *Tapestry* to ensure they know how to contact, teach and support pupils and parents in the event of a school closure (please see our **Remote Education Policy** for more information).

**The Online Safety Lead** (who is a trained trainer) will undertake Child Protection and Safeguarding training, which will include Online Safety, at least every 2 years. They will also update their Online Safety knowledge and skills at regular intervals, and at least annually.

**Governors** will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

**Volunteers** will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our **Child Protection and Safeguarding Policy**.

## 8.2 Educating Pupils about Online Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the School's safeguarding provision.

These skills and competencies are taught within the curriculum so that pupils have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Pupils should know how to deal with any incidents with confidence, as we adopt a 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Pupils will also leave school with clear knowledge and understanding of what they should and should not post or upload online, including personal details that give clues or indications of where they may live, travel to or who they spend time with.

Students will have access to *Google Classroom* for class collaboration across all subjects, and will each be given a personal Google email account. In order to ensure safeguarding procedures are met, these email accounts are unable to send and receive messages from external email addresses. Pupils are expected to use their email addresses appropriately and only as directed by a teacher; not as a chat function to communicate with other pupils.

The safe use of social media and the internet will also be covered in other subjects where relevant.

The School will raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

In **Key Stage 1**, pupils will be taught to:

- use technology safely and respectfully, keeping personal information private
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of Primary School**, pupils will know:

- that people sometimes behave differently online, including pretending to be someone they are not
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online even when we are anonymous



- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- how to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- how information and data is shared and used online
- how to respond safely and appropriately to adults they do not know, whom they may encounter in all contexts, including online
- how to identify warning signs that a website may not be secure, including how to recognise false information

### 8.3 Educating Parents about Online Safety and Additional Support

As part of the approach to developing online safety awareness with pupils, All Saints' School offers parents the opportunity to find out more about how they can support the School in keeping their child safe and find out what they can do to continue to keep them safe whilst using online technologies beyond school. The School will raise parents' awareness of internet safety through consultation evenings, newsletters, letters, our website and information about national and local online safety campaigns and literature, and in information via our remote learning environment (*Tapestry* for Reception and *ClassDojo* for the rest of the School). This policy will also be shared with parents.

Following updates in *KCSiE* 2024, the School will also share information with parents/carers about:

- what systems we have in place to filter and monitor online use
- what we are asking pupils to do online, including the sites they will be asked to access
- who from the School (if anyone) their child is going to be interacting with online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL/Online Safety Lead. Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

In the event of school closure, parents will have access to their designated online portal to support home learning (*ClassDojo* for KS1 and KS2; *Tapestry* for Reception). It is the responsibility of Class Teachers to support parents on these online portals, but the Online Safety Lead will monitor and support teachers where possible. See the **Remote Education Policy** for further detail.

The School wishes to promote a positive attitude to using the internet and therefore would like parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

## 9. Links to Other Documents and Policies

This **Online Safety and Acceptable Use Policy** is linked to our **Computing Intent Document, Privacy Notices** (sent to families with induction packs when they join the School) as well as the following policies (see the **Documents and Policies Library** on our website):

- [Anti-Bullying Policy](#)
- [Behaviour Policy](#)
- [Child Protection and Safeguarding Policy](#)
- [MAT Complaints Procedure](#)
- [MAT Data Protection Policy](#)
- [MAT Relationships and Sex Education Policy](#)
- [Mobile Phone Policy](#)
- [Remote Education Policy](#)



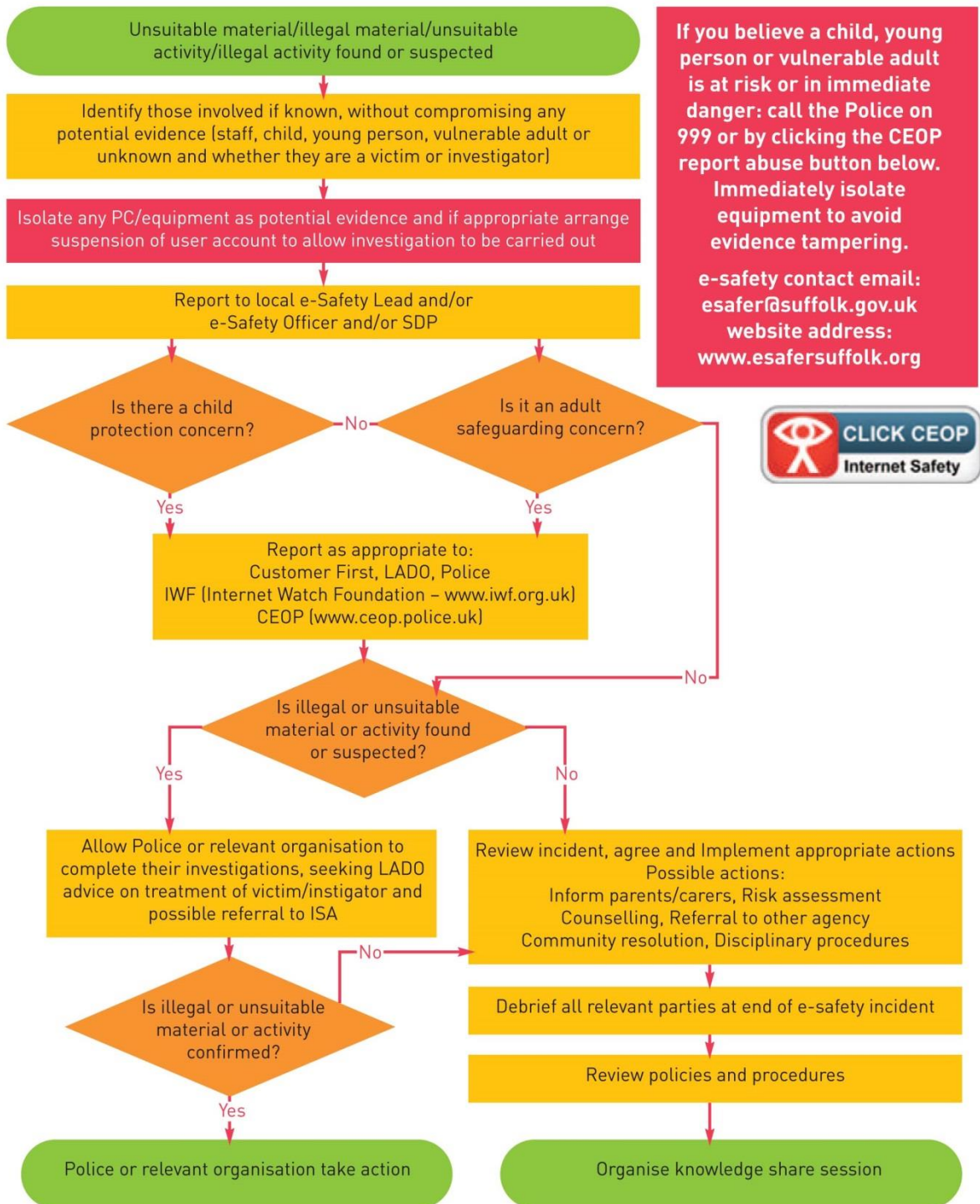


## Appendix 1: Online Safety Training Needs – Self Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
<b>Question</b>	<b>Yes/No (add comments if necessary)</b>
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for Staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

## Appendix 2: E-Safety Incident Flowchart

# e-Safety Incident Flowchart



### Appendix 3: Acceptable Use Agreement for Staff, Governors and Visitors

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the School must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to pupils for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- 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 pupils before they can upload images (video or photographs) to the internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of pupils if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise effectively.
- I will report accidental misuse.
- I know who my Designated Safeguarding Lead, Alternate DSLs and Online Safety Lead are.
- I will report any incidents of concern for a pupil's safety to the Headteacher, DSL or Online Safety Lead in accordance with procedures listed in the **Online Safety Policy**.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact pupils via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones (if provided) and only to a pupil's school e-mail address upon agreed use within the School.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher and/or Online Safety Lead.
- 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.
- I know that I should use the encrypted laptop and memory stick provided by the School for all school-related data. Should I use a personal device I am aware that this must also be encrypted. All devices holding school-related data should be kept securely at all times and not be left in open places in school, at home or in cars.
- If I bring my mobile phone, or other personal device, into school I know that this must be password protected.
- I will ensure that I follow the GDPR procedures and will check if I am unsure.

I will ensure that I keep my password complex and secure, and change it half-termly. I will log-off whenever I am leaving the room and will not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Online Safety Lead prior to sharing this information.

- I will adhere to copyright and intellectual property rights.
- 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.
- I have been given a copy of the **Online Safety Policy** to refer to about all Online Safety issues and procedures that I should follow.
- I have read, understood and will adhere to the Principles outlined in the **Social Media Policy**.

I have read, understood and concur with this Agreement as I know that by following this I have a better understanding of Online Safety and my responsibilities to safeguard pupils when using online technologies. I understand that if I break any of these rules disciplinary procedures will apply.

Signed.....Date.....

Name (printed).....

## Appendix 4: ICT Class Agreement

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school email address when emailing in school.
- I will not be accessing my *Google Classroom* account from home at this time.
- I will only open email attachments from people I know, or whom my teacher has approved.
- I will not tell other people my ICT passwords/log-ins.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school activity approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Signed by:

Date: September 2023

## Appendix 5: Pupil and Parents' Online Safety Agreement

### All Saints' C E Primary School, Newmarket

#### Pupil and Parents' Online Safety Agreement

As a pupil, you use computer facilities including Internet access as an essential part of your learning, as required by the National Curriculum.

##### As a pupil at All Saints' C E Primary:

- I have read/listened to and understood the Think Then Click (KS1) or SMART Online Safety Rules (KS2).
- I will use the Internet to help me learn.
- I agree to use the computer, network, Internet access and other new technologies in a sensible way at all times.
- If I need help, I know who I can ask and that I can go to [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) for help if I cannot talk to a trusted adult.
- I know that my computer and Internet browsing will be checked.
- I understand that if I deliberately break the rules, I could be stopped from using the Internet or computers.
- I will abide by the SMART Online Safety Rules when on social media outside of school.

##### As a parent/carer of a pupil in All Saints' C E Primary:

- I have read and understood the school Online Safety rules and **give permission for my child to access the internet in school.**
- I understand that the school will take necessary precautions (filtering and monitoring is in place) to ensure that pupils cannot access inappropriate materials, but appreciate this is a difficult task.
- I understand that the school cannot be held responsible for the content of materials accidentally accessed through the internet.
- I agree that the school is not liable for any damages arising from the use of internet facilities.
- I agree not to name pupils or All Saints' Staff on the internet without permission, or in a derogatory way.

### KS1 Internet Rules

# KS1 Think then Click



**These rules help us stay safe on the Internet**








- We only access the Internet when an adult is with us
- We can click on the links when we know what they do
- We can search the Internet with an adult
- We always ask if we get lost on the Internet







## KS2 SMART Online Safety Rules

 <b>Safe</b>	<p>Keep safe by being careful not to give out personal information when you're chatting or posting online.</p> <p>Personal information includes your full name, photos, home address, email address, phone number and passwords.</p> 
 <b>Meet</b>	<p>Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and, even then, only when they can be present.</p> <p>Remember online friends are still strangers even if you have been talking to them for a long time.</p>
 <b>Accepting</b>	<p>Accepting emails, IM messages, or opening files, images or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!</p>
 <b>Reliable</b>	<p>Someone online might lie about who they are and information on the internet may not be true.</p> <p>Always check information by looking at other websites, in books, or with someone who knows.</p> <p>If you like chatting online it's best to only chat to your real world friends and family.</p> 
 <b>Tell</b>	<p>Tell a parent, carer or a trusted adult if someone, or something, makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.</p>