Wyburns Primary School

Online Safety Policy

Date Policy Created	October 2025
Reviewed by Governors	October 2025
Next Review	October 2026

Our school works in accordance with the PREVENT Duty and approaches this issue in the same way as any other child protection matter. Any concerns that one of our pupils is at risk in this respect, will be referred to Children's Social Care in line with the SET procedures.

Wyburns Primary School is a Rights Respecting School. Our policies are underpinned by the UNCRC.

Article 29(goals of education) Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, and the environment.

Equality and Inclusion

At Wyburns Primary School, we are committed to ensuring equality of education and opportunity for all pupils, staff, parents and carers; irrespective of age, race, gender, disability, faith or religion, attainment or socio-economic background. We aim to develop a culture of inclusion and diversity in which all those connected to the school feel proud of their identity and able to participate fully in school life.

The achievement of all pupils is monitored and we use this data to support pupils, raise standards and ensure inclusive teaching. We will tackle discrimination by the positive promotion of equality, challenging bullying and stereotypes and creating an environment which promotes British values; championing respect for all.

We believe that diversity is a strength, which should be respected and celebrated by all those who learn, teach and visit here. As an educationally inclusive school the teaching and learning, achievements, attitudes and well-being of every young person matters.

Our Mission Statement for Equality:

As a school,

- We welcome our duties under the Equality Act 2010 to eliminate discrimination, advance equality of opportunity and foster good relations in relation to age, disability, ethnicity, gender (including issues of transgender, and of maternity and pregnancy), religion and belief, and sexual identity.
- We welcome our duty to promote community cohesion.
- We recognise these duties reflect international human rights as expressed in the UN Convention- The Rights of the Child.

Introduction

Computing is an essential resource to support learning and teaching; as well as playing an important role in the everyday lives of children, young people and adults.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

The purpose of this policy is to:

- Have robust processes in place to ensure online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear procedures to identify, intervene and escalate an incident, where appropriate.
- To help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.

At Wyburns, we believe that online safety is an essential part of safeguarding and that it is our duty to ensure that all learners and staff are protected from potential harm online. We understand the responsibility to educate our pupils in online safety issues; teaching them appropriate behaviours, helping them to build resilience, developing strategies to manage and respond to risk online and the critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. We acknowledge that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. Staff should be particularly aware of pupils who may be more vulnerable, e.g. SEND pupils, pupils who are at risk of radicalisation.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, portable media players, etc.)

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites/ Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Artificial Intelligence (AI)
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting/ Video Podcasting

- Music Downloading/ Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

1. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools, including:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Head of Schools and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Meeting Digital and Technology Standards in Schools

It also refers to the DfE'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.

2. Roles and Responsibilities

2.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Head of School to account for its implementation.

The governing board 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).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

2.2 The Head of School

The Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The Head of School will use Surf Protect daily to identify if inappropriate internet access has been sought, and who by.

2.3 The Designated safeguarding lead

Details of the school's DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary.This list is not intended to be exhaustive.

2.4 The Computing Lead

The computing lead is responsible for:

- Updating and delivering staff training on online safety
- Providing reports on online safety in school to the head of school and/or governing board
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

2.5 The ICT consultant

The ICT provider is responsible for:

- Putting in place appropriate filtering and monitoring systems on school networks and devices, 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The above lists are not intended to be exhaustive.

2.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL and computing lead to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Protecting children from maltreatment, whether that is within or outside the home, including online and all incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

2.7 Parents

Parents are expected to:

- Notify a member of staff or the Head of School of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- 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
- Advice & Control setting - Internet Matters

2.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

3. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum and following the eight aspects from the Education for a connected world Framework. This is delivered to the children by using the Project Evolve toolkit.

The text below is taken from the National Curriculum computing programmes of study.

Under the new requirement, all schools will have to teach:

- Relationships education and health education in primary schools
- This new requirement includes aspects about online safety.

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 by 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 including 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 may encounter (in all contexts, including online) whom they do not know*

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

Online Safety and Children with Additional Needs

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues. Consideration is given to this when planning.

Class Environment

All classrooms will have Online safety posters for their Key Stage displayed (Appendix 5). At the beginning of each school year the children's Acceptable Use Agreement (Appendices 1 &2) is discussed as a class and all the children sign it to say they agree. This is also displayed in the classroom and referred to throughout the year.

4. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head of School.

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as 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 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.

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 14 for more detail).

The school also gives information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes 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.

5.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been 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's code of conduct/ acceptable use policy

If inappropriate or potentially illegal material is found on a device, the staff member must inform the DSL immediately.

- If the material is illegal, the DSL must retain the material as evidence and report the matter to the police. Deleting the material is not permitted.
- If the material is inappropriate but not illegal, the DSL and staff member will decide whether to:
    - delete it,
    - retain it as evidence for a behaviour or safeguarding concern, and/or
    - take further action in line with school procedures.

Any searching of pupils will be carried out in line with the DfE's latest guidance on Searching, Screening and Confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to follow the agreement regarding the acceptable use of the school's computing systems and the internet (appendices 1-2). Visitors will

be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2

7. Social Media

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites. Some with the widest use are Instagram, Facebook, X and Tic Tock. The widespread availability and use of social networking applications brings opportunities to understand, engage and communicate with audiences in new ways. However, it is important to ensure that we balance this with our reputation. The use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

Social networking applications include, but are not limited to:
Blogs, for example Blogger
Online discussion forums, such as netmums.com
Collaborative spaces, such as Facebook Media sharing services, for example
YouTube 'Micro-blogging' applications, for example X

All school representatives should bear in mind that information they share through social networking applications, even if they are in private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

The way in which school staff present and conduct themselves on social networking sites can have an impact on the public perception of the school and influence the way in which those staff members are perceived by pupils and parents of the school. In their use of social networking sites, staff should be aware that their online behaviour could affect their professional standing, dignity and perception of their integrity. School staff must take adequate precautions when using social networking sites/applications, both in vetting material that could be connected to them (through their own profile and information added about them) and through the use of appropriate security settings.

7.1 Use of Social networking sites in worktime

Use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Head of School.

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head of School or a member of the SLT first.

7.2 Social Networking Terms of Use

Social Networking applications:

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.

- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with. This could be viewed as a safeguarding issue.
- Employees should not identify themselves as a representative of the school as this could directly link their behaviour outside of work with the reputation of the school.
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head of School
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally affects the employer's reputation then the employer is entitled to take disciplinary action.

7.3 Guidance/protection for staff on using social networking

- No member of staff should interact with any pupil in the school on social networking sites. This could be viewed as a safeguarding issue.
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18
- This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in school and there are legitimate family links, please inform the head teacher in writing. However, it would not be appropriate to network during the working day on school equipment
- It is illegal for an adult to network, giving their age and status as a child
- If you have any evidence of pupils or adults using social networking sites in the working day, please contact the DSL.

7.4 Guidance/protection for Pupils on using social networking

- No pupil under 13 should be accessing social networking sites. This is the guidance from Facebook. There is a mechanism on Facebook where pupils can be reported via the Help screen.
- No pupil may access social networking sites during the school working day
- All pupil mobile phones must be handed into the office at the beginning of the school day, the Internet capability must be switched off.
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head of School. Parents will be informed if this happens
- No school computers are to be used to access social networking sites at any time of day

8. Personal Mobile devices in school and on school trips

8.1 Pupils using mobile devices in school and on school trips

Pupils walking home alone may bring mobile devices into the school, but are not permitted to use them on-site. Pupils store mobile devices in the office or a secure box in the classroom at their own risk, and the school takes no responsibility for the security of these devices. The internet capability must be switched off.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1)

Any breach of the acceptable use agreement by a pupil may result in the confiscation of their device.

8.2 Staff with mobile devices in school and on school trips

- Staff are not permitted to make/receive calls/texts during contact time with children, unless by prior arrangement with the Head of School.
- Emergency contact should be made via the school office.
- Staff should have their phones on silent or switched off and out of sight during class time.
- Mobile phones can be used during break and lunchtimes but should not be used in a space where children are present.
- Staff personal mobiles must be password protected so that they cannot be used if found by a child.
- Staff are not permitted to use recording equipment on their mobile phones to take recordings of children or to share images of the pupils.
- During a trip, it may be necessary for a staff member to use their own mobile phone to call the school directly.

8.3 Parents/ visitors with mobile devices in school and on school trips

- Parents are only allowed to photograph or video school events such as shows or sports day using their mobile phones if directed that they can do so by the Head of School. The school will insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own. If there are pupils present that the school does not have permission to photograph then all photos and recordings will be prohibited due to safeguarding.
- Where parents/volunteers are accompanying school trips they should not use their mobile phone in the presence of children.
- Parents/ volunteers on school trips are informed not to make contact with other parents (via calls, texts, email or social networking) during the trip.
- Parents / volunteers should not use their phone to take photographs of children on school trips.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – all Wyburns' devices contain the Bios password which secures the device if lost or stolen
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

- All Wyburns' devices are protected by Sophos antivirus – that updates every hour on the hour.
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from our Computing Consultant; Ryan Summerhayes and inform the Head of School.

10.

Emails

The use of email is essential. In the context of school, e-mail should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette; ('netiquette').

10.1 Managing Emails

- The school gives all staff their own email account to use for all school business as a work-based tool.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending curriculum-based emails to external organisations are advised to cc. their line manager or Head of School.
- Staff sending emails to parents should do so via the school office.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- All pupil email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Staff must inform the Head of School if they receive an offensive email
- However, staff access their school email (whether inside or outside of school) all the school email policies apply

10.2 Sending Emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section below *'Emailing Personal, Sensitive, Confidential or Classified Information'.*
- All stakeholders in the school must use their own school email account so that they are clearly identified as the originator of a message
- An outgoing email greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming email
- School email is not for personal use.

10.3 Receiving Emails

- Staff are asked to check their email regularly
- Never open attachments from an untrusted source; consult the network manager first if you have any concerns

10.4 Emailing Personal, Sensitive, Confidential or Classified Information

- Staff should assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided wherever possible unless password protected.
- The use of Hotmail, BT Internet, AOL or any other internet based webmail service for sending e-mail containing sensitive information is not permitted

Where the conclusion is that email must be used to transmit such data:

- Obtain express consent from the Head of School to provide the information by email before doing so
- Exercise caution when sending the email and always follow these checks before releasing the email:
    - Verify the details, including accurate email address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to email requests for information
    - Do not copy or forward the email to any more recipients than is absolutely necessary
    - Do not send the information to anybody/person whose details they have been unable to separately verify (usually by phone)
    - Send the information as an encrypted document attached to an email
    - Provide the encryption key or password by a separate contact with the recipient(s) – preferably by telephone
    - Do not identify such information in the subject line of any email
    - Request confirmation of safe receipt.

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Essex Police

- District and Borough Councils within Essex County Council
- Essex NHS Trusts

11. The Internet Managing the Internet

- The school maintains students have supervised access to Internet resources through the school's fixed and mobile internet technology
- Staff preview any recommended sites before use with pupils
- www.viewpure.com is used to show any online videos to pupils. Alternatives are, www.watchkin.com and www.safeshare.tv
- Staff are to encourage pupils to use a 'child-friendly' search engine such as 'Kiddle' when conducting research.
- Parents are advised to check sites and supervise their child's work when they are researching online.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Stakeholders in the school should not reveal any confidential information of pupils, parents/carers, staff, governors or anyone linked to the school through an outside agency on any social networking site or blog
- Online gambling or gaming is not allowed using technologies provided by the school or personal technologies whilst on school property.
- Staff should only download personal data from systems if expressly authorised to do so by the Head of School.
- Stakeholders in the school must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Staff should keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information.
- Staff should ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

11.1 Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- The school ensures that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access

12. Images

12.1 Safe Use of Images - Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. All staff are aware that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment (e.g. teacher ipads)
- Personal digital equipment, such as mobile phones and cameras must not be used to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others whilst in school, unless with express permission of the Head of School and under supervision.

12.2 Consent of Adults Who Work at the School

Permission to use images of all staff who work at the school is sought.

12.3 Publishing Pupil's Images

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's photos in the following ways:

- On the school website
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- On social media sites

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Only the Web Manager, Head of School, teachers and the office administrator have authority to upload pupil images to the school website.

12.4 Storage of Images and videos

- Images/ films of children are stored on the school's network – Staff Shared, not Google.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head of School
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.
- Images are deleted when they are no longer required, or the pupil has left the school

- Images may be stored temporarily on teacher ipads / laptops that are secured by passwords

13. How the school will respond to issues of misuse

Where a pupil misuses the school's computing systems or internet, we will follow the procedures set out in our behaviour policy. 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 code of conduct policy. 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.

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

An incident report log can be found in appendix 4.

16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Computing policy

Appendix 1

Acceptable Use Agreement

This is how we stay safe when we use computers:

EYFS and Keystage 1

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me or I think is wrong on the screen.
- I know that if I break the rules I might not be allowed to use a computer/tablet.

Keystage 2

- I will only use IT in school for school purposes.
- I will not tell other people my IT passwords.
- I will not give out my own details such as my name, phone number, school or home address.
- I will only open/delete my own files.
- I will only open email attachments under direct instruction from my teacher
- I will make sure that all IT contact with other children and adults is responsible, polite, sensible and legal.
- 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 know that what I type in a search engine is filtered, monitored and reported.
- I know that my use of IT can be checked and that my parents/carer will be contacted if a member of school staff is concerned about my online safety in school or at home.
- I will not arrange to meet anyone in person from contact made on social media.
- I will treat people I meet online as strangers and not friends.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.

Date: _____

Appendix 2

Acceptable Use Agreement for staff, governors, volunteers and visitors.

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This acceptable use agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

All staff are expected to sign this agreement and adhere at all times to its contents.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable).

I will not:

- Use them in any way which could harm the school's reputation
- 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)
- 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
- Use my personal phone during teaching times
- Take photographs of pupils on a personal device
- Take photographs/share images of pupils unless parental consent has been granted
- 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 and permission has been given by the Head of School

I will:

- Read and fully understand the school Online Safety Policy, Data Protection Policies and Safeguarding Policy.
- Only use the school's ICT systems and devices whilst in school.
- Only use a work device to access the internet outside of school if it is for educational purposes or for the purpose of fulfilling the duties of my role.
- Agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- 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.
- Lock my computer if it's logged in when I leave it, unless in a secure room.
- Let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others
- Let the DSL know if I inadvertently access illegal pornographic material, even if on my own devices.
- Always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I understand that the school's devices and networks have a filtering and monitoring system in place and any inappropriate actions may be recorded and notified to the Head of School.

IT Acceptable User Agreement

I have read, understood and agree to follow the school's policies and guidelines with regards to using school ICT devices, networks and systems, whether in school or out of school.

I understand that personal devices are not to be used in school - with the exception of my phone for emergency or educational purposes if I am in the staffroom or as part of my role expectations. My phone should never be accessible to others and should be locked if not in use.

Date: .....

Full Name (printed): .....

Appendix 3a

Flowchart responding to incidents of misuse

Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an illegal e-safety incident

YES

Inform Essex Police and Essex County Council

Follow the advice given by the Police, or

Confiscate the device and if related to the school network disable user account

Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

If a pupil is involved contact Social Care Direct to make an emergency referral on 0845 603 7634

If it involves a member of staff contact the LADO on 01245 436744

NO

Go to next flowchart which outlines the process for non-illegal incidents

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

Examples of illegal activity would include:

- Downloading abusive images
- Passing child pornography to others
- Inciting racist or religious hatred
- Extreme cases of cyberbullying
- Promoting illegal acts

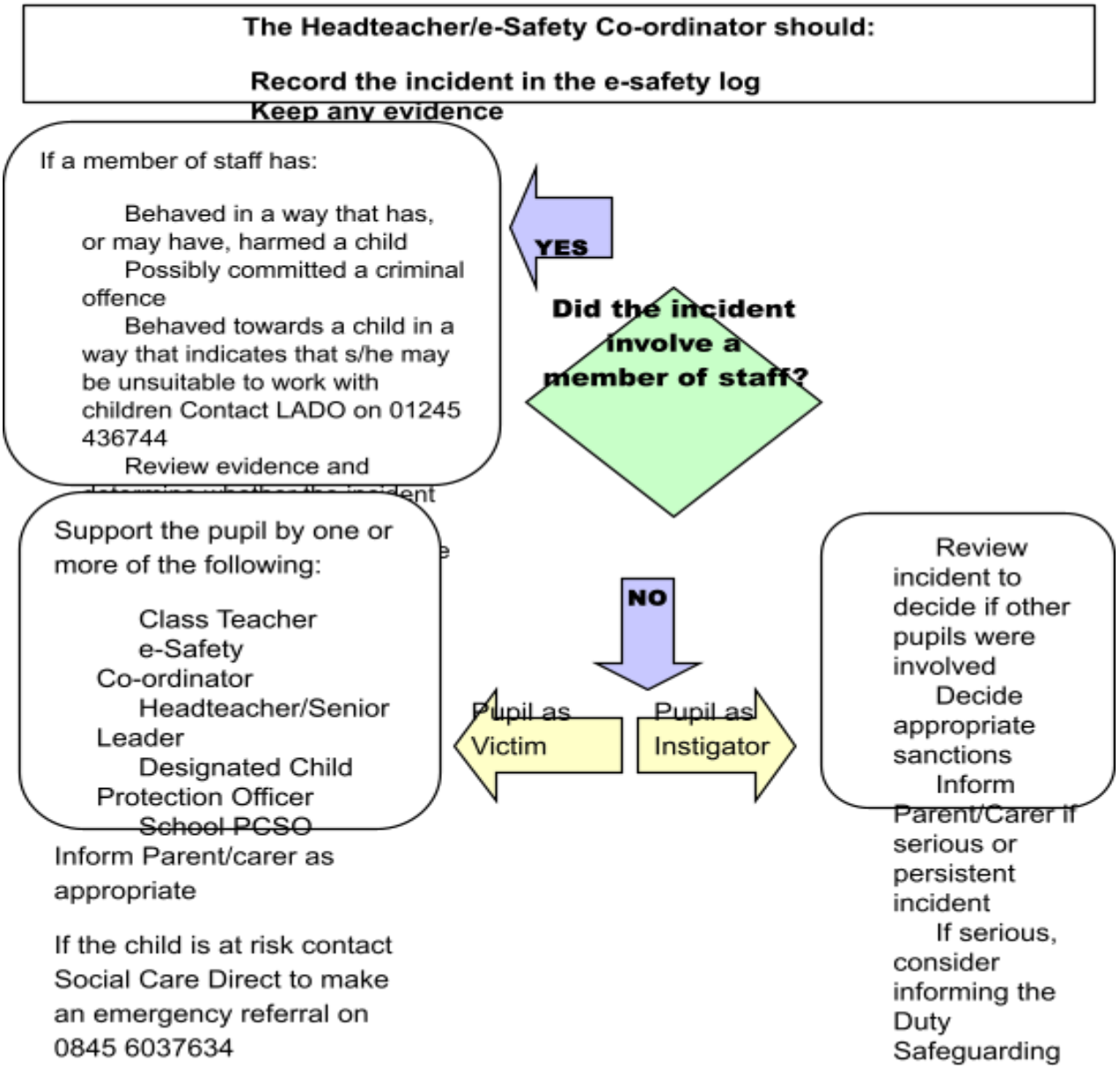
Still unsure?

For further advice ECC ISIS helpdesk on 01245 431851 or Essex Police on 0300 333 4444

Appendix 3b

Flowchart responding to incidents of misuse

Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to where no illegal activity has taken place.



Non-illegal incident types could be:

- Using another persons user name or password
- Accessing websites which are against the schools policy e.g. gaming
- Using a mobile phone to take a video during a lesson
- Using technology to upset or bully

Appendix 5a

Classroom Online Safety

Poster EYFS and KS1

Classroom Online Safety

Poster KS2