Schools for Every Child

Shared Moral rooting- *The driving force that gives ethical and moral validity to the organisation. A higher purpose that can be relied upon to drive the organisation. A rooting is long lasting and outlives the wishes of one individual or another.*

- *UNICEF rights of child*

Shared Values- *Actions and things we do day to day; we live our values to get to our vision:*

- ***Altruistic-*** *Doing good things whenever, however and to whoever you can*
- ***Pioneering-*** *striving to discover new things and exceed expectations*
- ***Ethical-*** *Making conscious decisions to be kind and fair*

Shared Vision- *an aspiration for the future. This holds the different parts of the organisation together. The shared vision is something each part works towards, in its own way. Specific enough that it stands you apart from others in the same field.*

- ***Nurturing Brilliance, Guiding Exploration, Cultivating Respect-*** *a committed journey to put every learner's individuality, curiosity, and dignity at the forefront of the world that awaits.*

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

UNICEF Article 28(right to an education)

· *Every child has a right to an education. Children's human dignity. Wealthy countries must help poorer countries achieve this. 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.*

Date Policy Created	September 2017
Reviewed:	October 2026

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.

The purpose of this policy is to:.

- Have robust processes in place to ensure the 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 mechanisms 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.

Wyburns believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. Additionally, we believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online. 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
- 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 on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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 headteacher 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 teacher

The Head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

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 Computing Lead

The computing lead (Mrs J Franko/ Mrs L Hogan) is responsible for:

- Updating and delivering staff training on online safety
- Providing regular reports on online safety in school to the head teacher 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 manager

The ICT manager, Ryan Summerhayes 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

2.5 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.

This list is not intended to be exhaustive.

2.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher 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
- Healthy relationships – Disrespect Nobody

2.7 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:

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*

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 e-safety issues. Consideration is given to this when planning.

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 or Google Classroom. This policy will also be shared with parents.

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

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

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 11 for more detail).

The school also sends information/leaflets 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 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.

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. Pupils using mobile devices in school

Pupils (in years 5 and 6) 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.

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 trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

8. 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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- 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 Miss C Harrison (Computing Lead)

9. Emails

The use of e-mail is essential. In the context of school, e-mail should not be considered private. Educationally, e-mail 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 e-mail in relation to their age and good network etiquette.

Managing Email

- The school gives all staff their own e-mail 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 e-mail 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 e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending curriculum based e-mails to pupils or emails to external organisations are advised to cc. the Headteacher or line manager. Staff should only send curriculum based emails to pupils. 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 e-mail 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 Headteacher if they receive an offensive e-mail
- However staff access their school e-mail,(whether inside or outside of school) all the school e-mail policies apply

Sending Emails

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

Receiving Emails

- Staff are asked to check their e-mail regularly
- Never open attachments from an untrusted source; Consult the network manager first.

Emailing Personal, Sensitive, Confidential or Classified Information

- Staff should assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided wherever possible unless password protected.
- The use of Hotmail, BTInternet, AOL or any other internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where the conclusion is that e-mail must be used to transmit such data:

- Obtain express consent from the Headteacher to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any body/person whose details they have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- 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 e-mail
- 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

10. Internet Use

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
- Staff are to encourage children to use a 'child- friendly' search engine such as kiddle, when conducting research.
- Parents will be advised to supervise any further research
- 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 Headteacher
• 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.

10. 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.

11. 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Computing and internet acceptable use policy

Appendix 1: EYFS, KS1 and KS2 acceptable use agreement (pupils and parents/carers)

Being Safe Online



T - is it true?
H - is it helpful?
I - is it inspiring?
N - is it necessary?
K - is it kind?

Acceptable Use of Computing Equipment

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make other upset
- I will immediately inform an adult if I see something that worries me.
- I will keep all of my usernames and passwords secure. I will not share these with others.
- I understand not to share personal information, such as: phone numbers, address, birthday etc.
- I will respect computing equipment and notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools carefully and follow instructions from adults. I will only use these tools while supervised by an adult.
- I will T.H.I.N.K before I share or reply to anything online.
- In order to help keep me and others safe, I know that the school is able to check my files and my online activity.
- I understand that if I behave inappropriately while using technology, my parents/carers will be informed and appropriate action will be taken.

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

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:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

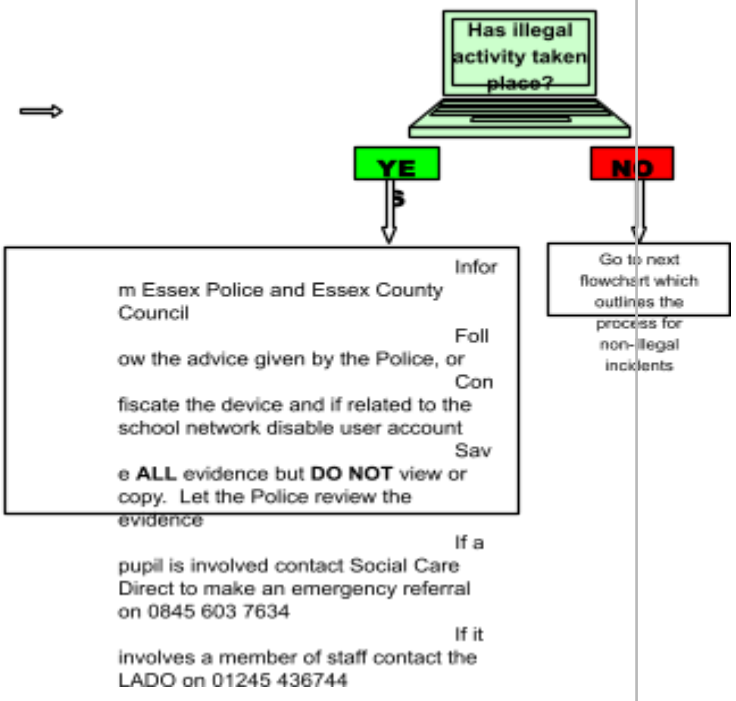
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

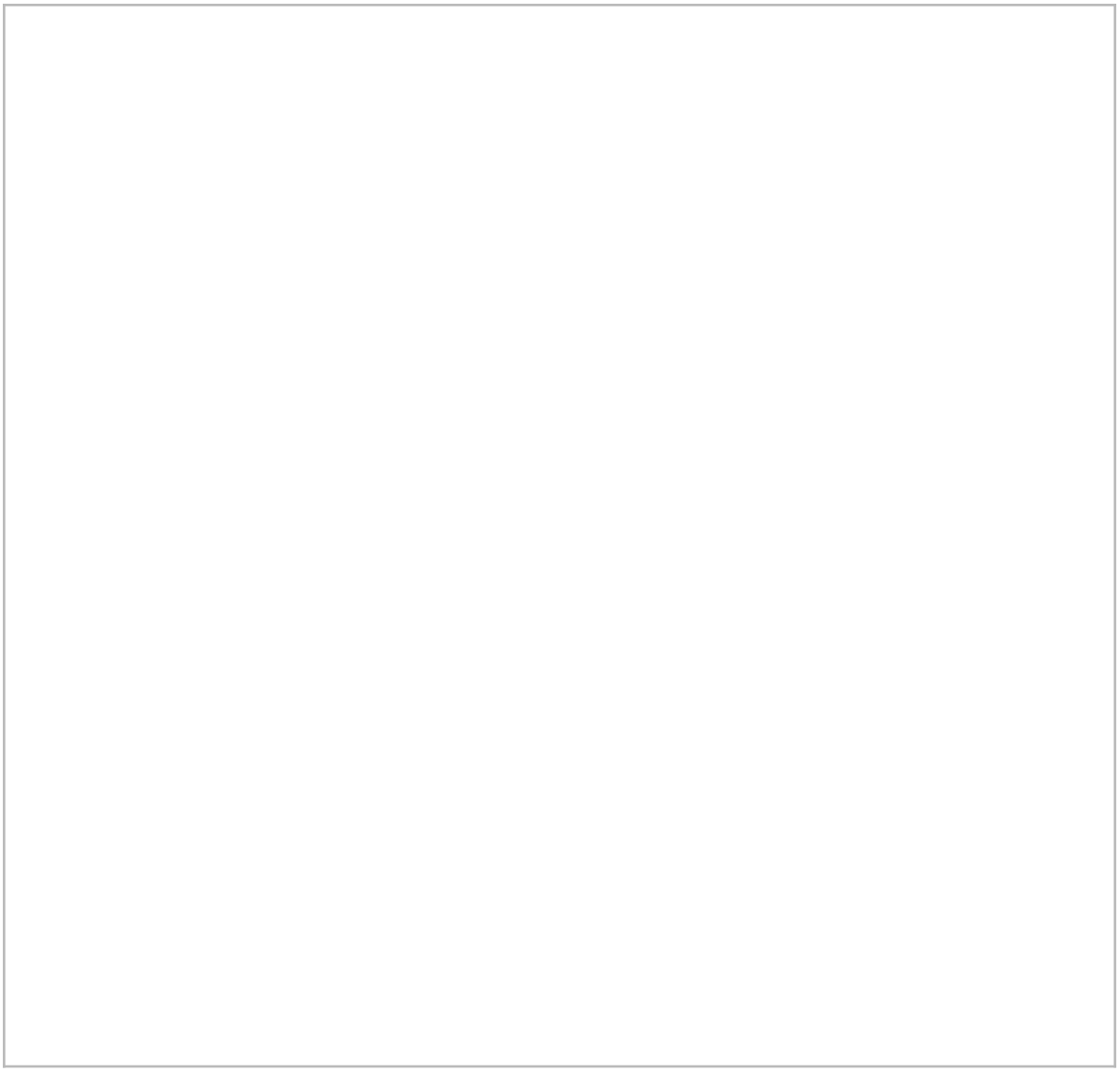
I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

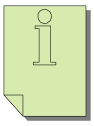




Appendix 3: Misuse Flow Chart

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

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?

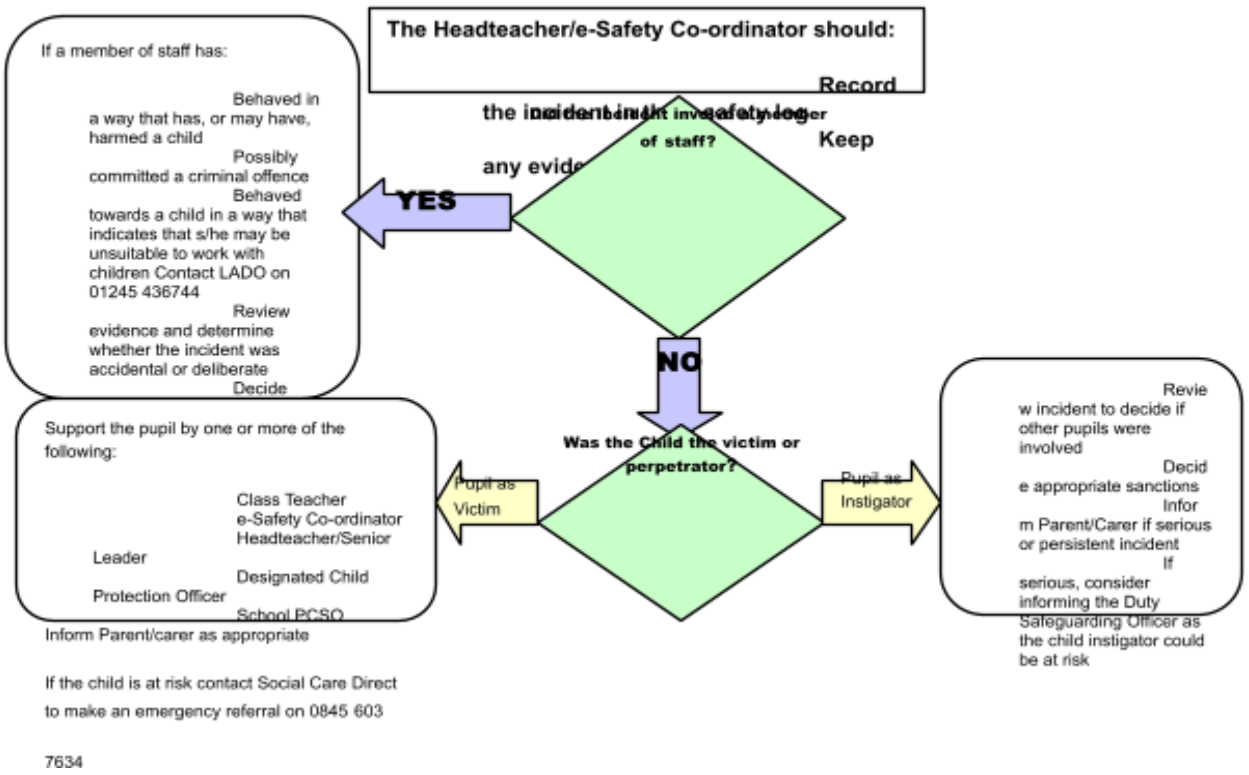
For further advice ECC ISIS helpdesk on

01245 431851 or

Essex Police on

0300 333 4444

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff



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

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 video during a lesson
- Using technology to upset or bully

Appendix 4: Online Safety Incidents Log (Found on Google Drive)

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 5: Online and Remote Teaching- FIO

(Remote learning):Safeguarding in schools, colleges and other education providers

Date of last review : March 24

Response to COVID-19/ School closure

There have been significant changes within our setting in response to the outbreak. Many young people are now at home and staffing is likely to be significantly affected through illness and self-isolation.

Despite the changes, the school's Online Safety Policy is fundamentally the same

This annex sets out some of the adjustments we are making in line with the changed arrangements in the school and following advice from government and local agencies.

Risk online

Young people will be using the internet more during this period. The school may also use online approaches to deliver training or support. Staff will be aware of the signs and signals of cyberbullying and other online risks and apply the same child-centred safeguarding practices as when children were learning at the school.

- The school continues to ensure appropriate filters and monitors are in place
- Our governing body will review arrangements to ensure they remain appropriate
- The school has taken on board guidance from the UK Safer Internet Centre on safe remote learning and guidance for safer working practice from the Safer Recruitment Consortium. We have reviewed the code of conduct and information sharing policy accordingly - information will only be shared with school staff as necessary for the setting of work.
- In case of school or bubble closure, live lessons will be available to all pupils affected. All live teaching will be through Google Meet or Zoom platforms.

- The use of Google Classroom and Zoom software will be constantly under review and revision by: The Trustees, CEO, heads and SLT
- Staff have discussed the risk that professional boundaries could slip during this exceptional period and been reminded of the school's code of conduct and importance of using school systems to communicate with children and their families.
- Staff have read the 20 safeguarding considerations for livestreaming.
- Children and young people accessing remote learning receive guidance on keeping safe online and know how to raise concerns with the school, Childline, the UK Safer Internet Centre and CEOP. Links to the CEOP learning package will be made available to parents though our website.

- Parents and carers have received information about keeping children safe online with peers, the school, other education offers they may access and the wider internet community. We have set out the school's approach, including the sites children will be asked to access and set out who from the school (if anyone) their child is going to be interacting with online. Parents have been offered the following links:
    - Internet matters - for support for parents and carers to keep their children safe online
    - London Grid for Learning - for support for parents and carers to keep their children safe online
    - Net-aware - for support for parents and carers from the NSPCC
    - Parent info - for support for parents and carers to keep their children safe online
    - Thinkuknow - for advice from the National Crime Agency to stay safe online
    - UK Safer Internet Centre - advice for parents and carers

- Free additional support for staff in responding to online safety issues can be accessed from the Professionals Online Safety Helpline at the UK Safer Internet Centre.

Protocol for using Zoom/Google Meet is as follows:
Pupils

By joining a live-stream they are:

- Complying with the platform's terms and conditions.
- Knowing that everything seen, said and written is recorded
- Agreeing to be appropriately dressed, protecting modesty. Pyjamas etc. are not appropriate
- Not live streaming in their bedroom
- Ensuring no inappropriate objects/images are visible
- raising of hands when wanting to ask a question
- not sharing any part of a live-stream or video lesson with any other party
- being polite and courteous
- Having a parent/carer present but not necessarily in the view of screen

Teachers will:

- Ensure all chats are in small groups
- Partake in 1:1 sessions in some individual circumstances, but where possible should be in small groups.
- Wear suitable and professional clothing, as well as anyone else in the household
- Be in an appropriate area of the house and where possible against a neutral background
- Conduct all sessions on Wyburns' account
- Record the live session to Wyburns' Google Cloud or a Wyburns' device.
- Share the record of live session with SLT if asked for.
- Delete the chat only when instructed to do so by a member of SLT.

- Follow all instructions outlined in the training videos.
  i.e. waiting room, locking chats and turning off settings etc.
- Follow the risk assessment
- Agree to Google Meet and Zoom's Terms and Conditions
- Ensure all conversations with the children are in an appropriate manner. They will not ask for passwords, change the software/app or meet offline.