Whittingham
C of E PRIMARY SCHOOL

Whittingham C of E Primary School
E (Online) Safety Policy

This policy was developed during the Spring Term 2021 and was ratified by Governors during Spring Term 2021. It will be reviewed ***annually*** in line with safeguarding policies such as Child Protections and Safeguarding.

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.
Summaries of the key legislation and guidance are available on:

- online abuse **learning.nspcc.org.uk/child-abuse-and-neglect/online- abuse**
- bullying **learning.nspcc.org.uk/child-abuse-and-neglect/bullying**
- child protection **learning.nspcc.org.uk/child-protection-system**
- **It also takes into account the DfE statutory guidance 'Keeping Children Safe in Education' , Early Years and Foundation Stage , 'Working Together to Safeguard Children'**

Our School Vision and Values

The children know these as the 3R's:
'Hand in hand together we will become resilient, respectful and responsible citizens of our community and the wider world.'

School Aims:

- To provide an open, secure and welcoming Christian environment for each pupil. This is expressed through daily worship which acknowledges the presence of God in our lives.
- To further develop and value the partnership that exists between school and the local churches, in particular, through sharing weekly worship and to encourage an appreciation of the Christian faith and a familiarity with the local Christian heritage.
- To care for each pupils' safety, happiness and well-being.
- To value our pupils as individuals, developing their ability to take responsibility for themselves and their actions, promoting confidence and self-esteem, and respect for others and their environment.
- To equip our pupils with the knowledge to make informed choices about having a safe and healthy lifestyle.
- To offer opportunities for our pupils to become involved in the daily life of the school and to prepare them to play an active role as citizens locally and in the wider world.
- To provide a learning environment, which is challenging and stimulating yet ordered and disciplined.
- To provide a broad and balanced curriculum, setting realistic targets for each pupil.
- To extend and reinforce our pupils learning, making expectations clear, and raising achievement levels.

Policy statement and principles
Whittingham C of E Primary School fully recognises its responsibility for safeguarding and promoting the welfare of children with regards to e and online safety

This policy is one of a series in the school's safeguarding portfolio which includes:

- Staff/pupil online communication – Acceptable Use Policy and User agreements
- Remote Learning Policy and Code of Conduct
- Mobile Phone Policy Statement
- Relationships, Sex and Health education* (RSHE)
- Behaviour and Anti Bullying

Intent

At Whittingham C of E Primary School, we believe that:

children and young people should never experience abuse of any kind

children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

the online world provides everyone with many opportunities; however, it can also present risks and challenges

we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online

we have a responsibility to help keep children and young people safe online, whether or not they are using Whittingham C of E's network and devices

all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse

working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

Impact

We will seek to keep children and young people safe by:

appointing an online safety coordinator [this may or may not be the same person as your nominated child protection lead]. The person who has this responsibility is Belinda Athey supported by DSL's Caroline Kennedy and Neil Charlton providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults as well as our acceptable use agreements for staff and pupils

supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others

supporting and encouraging parents and carers to do what they can to keep their children safe online

developing an online safety agreement for use with young people and their parents/carers (At Whittingham we call this Acceptable Use User Agreement)

developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person

reviewing and updating the security of our information systems regularly

ensuring that user names, logins, email accounts and passwords are used effectively

ensuring personal information about the adults and children who are involved in our

organisation is held securely and shared only as appropriate

ensuring that images of children, young people and families are used only after their written

permission has been obtained, and only for the purpose for which consent has been given

providing supervision, support and training for children, staff, governors and volunteers about online safety

examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

Implementation

Monitoring and Review

Technology in this area evolves and changes rapidly. This school will review this policy at least annually.

The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the Head teacher will be informed of online safety concerns, as appropriate.

The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

Any issues identified via monitoring will be incorporated into our action planning.

Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Belinda Athey, Headteacher, has lead responsibility for online (E) safety. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.
- Whittingham C of E Primary recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure parents are directed to online safety advice and information
- Provide information on a school's website for parents and the community
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety

training.

- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding .

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

- Identify students who are involved in cybercrime, or those who are technically gifted and talented and are at risk of becoming involved in cybercrime, and to speak to the DSL immediately.

It is the responsibility of the company managing the technical environment

(we purchase an SLA from NCC) to:

- Implement appropriate security measures as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm

online.

- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and Engagement Approaches

At Whittingham we will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

Ensuring education regarding safe and responsible use precedes internet access.

Including online safety in Personal, Social, Health and Economic (PSHE), Relationships Sex Health Education (RSHE) and computing programmes of study.

Reinforcing online safety messages whenever technology or the internet is in use.

Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.

Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.

Implementing appropriate peer education approaches.

Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable Learners

Whittingham C of E Primary recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

When implementing an appropriate online safety policy and curriculum Whittingham C of E Primary will seek input from specialist staff as appropriate, including the SENCO, Looked After Child (LAC) Designated Teacher.

Training and engagement with staff

We will:

Provide and discuss the online safety policy and procedures with all members of staff as part of induction.

Provide up-to-date and appropriate online safety training for all staff, including governors where relevant to their role on a regular basis, with at least annual updates. This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.

Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.

Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.

Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.

Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

Awareness and engagement with parents and carers

Whittingham C of E Primary recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

Providing information and guidance on online safety in a variety of formats.

This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days as well as on the school website, ‘blog’, Twitter and Facebook pages.

Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.

Requiring them to read our acceptable use policies and discuss the implications with their children.

Reducing Online Risks

Whittingham C of E Primary recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

Regularly review the methods used to identify, assess and minimise online risks.

Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.

Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom Use

We use a wide range of technology. This includes access to:

Chromebooks, ipads, laptops and other digital devices

Internet which may include search engines and educational websites

Learning platform/intranet

Email

Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of learners will be appropriate to their age and ability.

The children will have access to regular and up to date online (e) safety training as part of their wider curriculum.

Early Years Foundation Stage and Key Stage 1

Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

Key Stage 2

Learners will use age-appropriate search engines and online tools.

Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

Managing Internet Access

We will maintain a written record of users who are granted access to our devices and systems.

All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

We will carry our regular audits and audit activity to help identify pupils trying to access sites to establish any vulnerabilities and offer advice, support and react accordingly

Filtering and Monitoring

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Working alongside the ICT team at NCC they have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.

Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

Changes to the filtering and monitoring approach will be risk assessed by NCC with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy will be logged and recorded by NCC

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Filtering

Education broadband connectivity is provided through NCC.

The filtering system blocks all sites on the Internet Watch Foundation (IWF) list. Our system is monitored by Senseo and Lightspeed which is endorsed by NCC.

We work with NCC to ensure that our filtering policy is continually reviewed.

If learners discover unsuitable sites, they will be required to:

Turn off monitor/screen and report the concern immediate to a member of staff.

The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy)

The breach will be recorded and escalated as appropriate.

Parents/carers will be informed of filtering breaches involving their child.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as NCC, IWF, Northumbria Police or CEOP.

Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices.

This is achieved by:

Physical monitoring (supervision),

If a concern is identified via monitoring approaches the DSL or deputy will respond in line with the child protection policy.

All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

https://whittingham.eschools.co.uk/website/gdpr_1/370977 Full information can be found in our information security policy.

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

Virus protection being updated regularly.

Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.

Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.

Not downloading unapproved software to work devices or opening unfamiliar email attachments.

The appropriate use of user logins and passwords to access our network.

Specific user logins and passwords will be enforced for all but the youngest users. (Note: this should be in place for all except Early Years and Foundation Stage children and some learners with SEND)

All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy (this may also be covered in other policies)

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

From year Reception all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.

We require all users to:

Always keep their password private; users must not share it with others or leave it where others can find it.

Not to login as another user at any time.

Managing the Safety of our Website

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

The administrator account for our website will be secured with an appropriately strong password.

We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

> The forwarding of any chain messages/emails is not permitted.
>
> Spam or junk mail will be blocked and reported to the email provider.
>
> Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
>
> Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell the Headteacher if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Staff email

Members of staff are encouraged to have an appropriate work life balance when responding to email or other such communication such as Tapestry and Class Dojo, especially if communication is taking place between staff, learners and parents. We encourage the use of 'quiet time' between 5.30 p.m. and 8.00 a.m.

Members of staff will refer to and adhere to the acceptable use policy and any other policy where staff use of mobiles is referred to.

Learner email

Learners may use provided email accounts for educational purposes.

Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

Whole-class or group email addresses may be used for communication outside of the setting.

Management of Learning Platforms (LP)

At Whittingham C of E Primary we use Tapestry and Class Dojo as its official learning platform.

Only current members of staff, learners and parents will have access to the LP.

When staff and/or learners leave the setting, their account will be disabled

Learners and staff will be advised about acceptable conduct and use when using the LP.

All users will be mindful of copyright and will only upload appropriate content onto the LP.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

The user will be asked to remove any material deemed to be inappropriate or offensive.

If the user does not comply, the material will be removed by the site administrator.

Access to the LP for the user may be suspended.

The user will need to discuss the issues with a member of leadership before reinstatement.

A learner's parents/carers may be informed.

If the content is illegal, we will respond in line with existing child protection procedures.

Social Media Expectations

The expectations' regarding safe and responsible use of social media and remote learning platforms applies to all members of our school community.

Members of staff will refer to and adhere to the schools social media policy and any other policy where the staff use of social media is referred to.

We will control learner and staff access to social media whilst using setting provided devices and systems on site.

Concerns regarding the online conduct of any member of Whittingham C of E Primary's community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Learners Personal Use of Social Media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.

We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not encourage the creation of accounts specifically for learners under this age and will not do this in school.

Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.

Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Learners will be advised:

To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.

To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.

To use safe passwords.

To use social media sites which are appropriate for their age and abilities.

How to block and report unwanted communications.

How to report concerns both within the setting and externally.

Official Use of Social Media

Whittingham C of E Primary's official social media channels are:

Twitter, Facebook

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher and Governors

Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

Staff use setting provided email addresses to register for and manage any official social media channels.

Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Use of Personal Devices and Mobile Phones (see separate policy)

Whittingham C of E Primary recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

Staff Use of Personal Devices and Mobile Phones (see separate policy)

Members of staff will refer to and adhere to the school's acceptable use policy and any other policy where the staff use of personal devises and mobile phones is referred to.

Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community will be made aware of the availability of the Cyber Choices early intervention programme for individuals who are involved in cybercrime, or those who are gifted and talented and are at risk of becoming involved in cybercrime.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.

Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and learners to work in partnership to resolve online safety issues.

After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

We will refer to the flow chart on responding to incidents, made available

Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or headteacher/manager will speak with Call Derbyshire/ Derbyshire Police first to ensure that potential investigations are not compromised.

Concerns about Learners Welfare

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.

The DSL (or deputy) will record these issues in line with our child protection policy.

The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Derby and Derbyshire Safeguarding Children Partnership thresholds and procedures.

We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

Our school leadership team has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education'.

Whittingham C of E Primary recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

We recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

Whittingham C of E Primary also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

Whittingham C of E Primary will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSHE curriculum.

We will ensure that all members of the community are aware of sources of support regarding

If made aware of online sexual violence and sexual harassment, we will:

Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.

Implement appropriate sanctions in accordance with our behaviour policy.

Inform parents and carers, if appropriate, about the incident and how it is being managed.

If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.

If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.

Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

Whittingham C of E Primary recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".

We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.

If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.

Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.

Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

Store the device securely.

If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.

Inform parents and carers, if appropriate, about the incident and how it is being managed.

Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.

Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

Whittingham C of E Primary will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

Whittingham C of E Primary recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community. There is also a 'Report a Concern' button on School 360.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

Act in accordance with our child protection policies and the relevant Safeguarding Child Board's procedures.

If appropriate, store any devices involved securely.

Make a referral to Children's Social Work Service (if required/appropriate) or 999 if a child is at immediate risk.

Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).

Inform parents/carers about the incident and how it is being managed.

Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Northumbria police by using 101.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to Northumbria police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).

If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Northumbria Police first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

Whittingham C of E Primary will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.

If made aware of IIOC, we will:

Act in accordance with our child protection policy and the relevant Safeguarding Children Partnership Safeguarding procedures (See Safeguarding Policy and E Safety Flowchart).

Store any devices involved securely.

Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Northumbria police or the DO (Designated Officer- See Safeguarding Policy).

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

Ensure that the DSL (or deputy) is informed.

Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

Ensure that any copies that exist of the image, for example in emails, are deleted.

Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

Ensure that the DSL (or deputy) is informed.

Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

Ensure that any copies that exist of the image, for example in emails, are deleted.

Inform Northumbria police via 101 (999 if there is an immediate risk of harm) and Children's Services using One Call (as appropriate).

Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

Ensure that the headteacher is informed in line with our managing allegations against staff policy immediately and without any delay.

Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.

Quarantine any devices until police advice has been sought.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at our school.

Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated and will be responded to in line with existing policies, including anti-bullying and behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The Police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through Northumbria police

Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and may include a referral into Channel.

If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Cybercrime

Cybercrime incidents and offences will be responded to in line with our existing behaviour policies.

We will respond to concerns that our students are involved, or at risk of becoming involved, in cybercrime, even if it takes place off site.

National Links and Resources for Educational Settings

CEOP:

www.thinkuknow.co.uk

www.ceop.police.uk

Childnet: www.childnet.com

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

Action Fraud: www.actionfraud.police.uk