Newnham St Peter's Church of England Primary School and Pre-School

SCHOOL POLICY

Policy name	**Online Safety**
Status	**Non-statutory**
Review period	**Annual**
To be read in conjunction with	**Safeguarding and Child Protection Policy** **Data Protection Policy** **Behaviour Policy with Anti Bullying and Hate** **Acceptable Use Agreement (included in policy)** **Staff Code of Conduct** **Remote Learning Policy**
Required on website	**Yes**

Review Progress

	Changes made? Y/N	*Name*	*Date*
Stage 1 – Ready for review		*A Nolan*	
Stage 2 - Governor review	*Y - see comments*		*10/10/2021*
Stage 3 – Completion by HT		A Nolan	28/10/21
Stage 4 - Adoption			

Related links

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
https://www.gloucestershire.gov.uk/media/2092529/gswp-may-2019-changes-highlighted.pdf (see paragraph127 and Annex D)
Actions for schools during the coronavirus outbreak - GOV.UK (www.gov.uk)
Safeguarding and remote education during coronavirus (COVID-19) - GOV.UK (www.gov.uk)
Undertaking remote teaching safely | NSPCC Learning

1.0 Aims

1.1 This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education', 'Early Years and Foundation Stage', 'Working Together to Safeguard Children' and Gloucestershire Safeguarding Children's Partnership Safeguarding procedures.

1.2 The purpose of this online safety policy is to:

1.2.1 Safeguard and protect all members of Newnham St Peter's C of E Primary School community online.

1.2.2 Identify approaches to educate and raise awareness of online safety throughout the community.

1.2.3 Enable all staff to work safely and responsibly, including in the delivery of remote learning, to role model positive behaviour online and to manage professional standards and practice when using technology.

1.3 Identify clear procedures to use when responding to online safety concerns.

1.4 This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

1.4.1 Content: being exposed to illegal, inappropriate or harmful material

1.4.2 Contact: being subjected to harmful online interaction with other users

1.4.3 Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

1.5 As a Church of England School we identify Christian values that underpin the whole of our community. These values inform our school's vision, aims and ethos, the design of our curriculum, all policies, planning and the school's management and governance. The value that relates particularly to this Policy is respect.

2.0 Policy Scope

2.1 Newnham St Peter's C of E Primary School 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.

2.2 Newnham St Peter's C of E Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

2.3 Newnham St Peter's C of E Primary School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

2.4 This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

2.5 This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptop, tablets or mobile phones.

3 Monitoring and Review

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

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

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

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

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

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

4 Roles and Responsibilities

4.1 The Designated Safeguarding Lead (DSL) Anne Nolan, Headteacher, has lead responsibility for online safety.

4.2 Newnham St Peter's C of E Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.3 The leadership and management team will:

4.3.1 Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.

4.3.2 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.

4.3.3 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.

4.3.4 Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.

4.3.5 Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.

4.3.6 Ensure parents are directed to online safety advice and information.

4.3.7 Provide information on a school's website for parents and the community.

4.3.8 Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.

4.3.9 Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
4.3.10 Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.4 The Designated Safeguarding Lead (DSL) will:
4.4.1 Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
4.4.2 Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
4.4.3 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.
4.4.4 Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
4.4.5 Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
4.4.6 Work with staff to coordinate participation in local and national events to promote positive online behaviour.
4.4.7 Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
4.4.8 Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
4.4.9 Report online safety concerns, as appropriate, to the Governing Body.
4.4.10 Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
4.4.11 Meet regularly with the governor with a lead responsibility for safeguarding.

4.5 It is the responsibility of all members of staff to:
4.5.1 Contribute to the development of online safety policies.
4.5.2 Read and adhere to the online safety policy and acceptable use policies.
4.5.3 Take responsibility for the security of setting systems and the data they use or have access to.
4.5.4 Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
4.5.5 Embed online safety education in curriculum delivery, wherever possible.
4.5.6 Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
4.5.7 Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
4.5.8 Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
4.5.9 Take personal responsibility for professional development in this area.
4.5.10 Identify students who are involved in cybercrime, or those who are at risk of becoming involved in cybercrime, and make a Cyber Choices referral.

4.6 It is the responsibility of the company managing the technical environment (ForestICT) to:
4.6.1 Implement appropriate security measures as directed by the DSL and leadership team to ensure that the setting's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

4.6.2 Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.

4.6.3 Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.

4.6.4 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.

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

4.7.1 Engage in age-appropriate online safety education opportunities.

4.7.2 Contribute to the development of online safety policies.

4.7.3 Read and adhere to the acceptable use policies.

4.7.4 Respect the feelings and rights of others both on and offline.

4.7.5 Take responsibility for keeping themselves and others safe online.

4.7.6 Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.8 It is the responsibility of parents and carers to:

4.8.1 Read the acceptable use policies and encourage their children to adhere to them.

4.8.2 Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.

4.8.3 Role model safe and appropriate use of technology and social media.

4.8.4 Abide by the acceptable use policies.

4.8.5 Identify changes in behaviour that could indicate that their child is at risk of harm online.

4.8.6 Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.

4.8.7 Contribute to the development of the online safety policies.

4.8.8 Use our systems, such as Seesaw and Teams, and other network resources, safely and appropriately.

4.8.9 Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5 Education and Engagement Approaches

5.1 The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

5.1.1 Ensuring education regarding safe and responsible use precedes internet access.

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

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

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

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

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

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

5.2.2 Implementing appropriate peer education approaches.

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

6 Vulnerable Learners

6.1 Newnham St Peter's C of E School 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.

6.2 Newnham St Peter's C of E School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
.

6.3 When implementing an appropriate online safety policy and curriculum Newnham St Peter's C of E Primary School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

7 Training and engagement with staff

7.1 We will:

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

7.1.2 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 update:

7.1.2.1. This will form part of the existing safeguarding and child protection training/updates as well as specific online safety sessions.

7.1.2.2 This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.

7.1.3 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.

7.1.4 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.

7.1.5 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.

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

7.1.7 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.

8 Awareness and engagement with parents and carers

8.1 Newnham St Peter's C of E School 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.

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

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

8.2.2 This will include offering specific online safety awareness training and highlighting online safety at other events such as parents' evenings, transition events, fetes and sports days.

8.2.3 Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
8.2.4 Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
8.2.5 Requiring them to read our acceptable use policies and discuss the implications with their children.

9 Reducing Online Risks

9.1 Newnham St Peter's C of E Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

9.2 We will:
9.2.1 Regularly review the methods used to identify, assess and minimise online risks.
9.2.2 Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
9.2.3 Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

9.3 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.

9.3 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.

10 Safer Use of Technology

Classroom Use
10.1 Newnham St Peter's C of E School uses a wide range of technology. This includes access to:
10.1.1 Computers, laptops and other digital devices
10.1.2 Internet which may include search engines and educational websites
10.1.3 Learning platform/intranet
10.1.4 Email
10.1.5 Digital cameras, web cams and video cameras

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

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

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

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

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

10.6.1 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.

10.6.2 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.

11 Managing Internet Access

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

11.2 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.

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

12 Filtering and Monitoring

12.1 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

12.2 Newnham St Peter's C of E School governors have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.

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

12.4 Changes to the filtering and monitoring approach will be risk assessed by ForestICT with educational and technical experience and, where appropriate, with consent from the leadership team;

12.5 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.

12.6 Education broadband connectivity is provided through swgfl.

12.7 The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

12.8 We work with ForestICT to ensure that our filtering remains secure.

12.9 If learners discover unsuitable sites:

12.9.1 They will be required to Turn off monitor/screen and report the concern immediate to a member of staff.

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

12.9.3 The breach will be recorded and escalated as appropriate.
12.9.4 Parents/carers will be informed of filtering breaches involving their child.
12.9.5 Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Gloucestershire Police or CEOP.

12.10 We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
12.10.1 Physical monitoring (supervision),

12.11 If a concern is identified via monitoring approaches:
12.11.1 DSL or deputy will respond in line with the child protection policy.
12.11.2 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.

13.0 Managing Personal Data Online

13.1 Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulation and Data Protection legislation. Full information can be found in our Data Protection Policy.

14.0 Security and Management of Information Systems

14.1 We take appropriate steps to ensure the security of our information systems, including:
14.1.1 Virus protection being updated regularly.
14.1.2 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.
14.1.3 Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
14.1.4 Not downloading unapproved software to work devices or opening unfamiliar email attachments.
14.1.5 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 Foundation Stage children and some learners with SEND). All users are expected to log off or lock their screens/devices if systems are unattended.
14.1.6 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.
14.1.7 From Pre-school all learners are provided with their own unique username and private passwords to access Seesaw. From Year One all pupils have their own email; learners are responsible for keeping their password private.
14.1.8 We require all users to:
14.1.8.1 Always keep their password private; users must not share it with others or leave it where others can find it.
14.1.8.2 Not login as another user at any time.

14.2 In the event of a cyber-attack:
14.2.1 All online equipment will be turned off immediately, including the school server.
14.2.2 ForestICT will be contacted to manage the cyber-attack and safely restore systems.
14.2.3 ForestICT will provide a full report to the school and the Governing Board.
14.2.4 The school will review practices and procedures in light of the report's findings.

15 .0 Managing the Safety of our Website

15.1 Our website is managed by Skyfire Designs.

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

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

15.4 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.

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

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

16.0 Publishing Images and Videos Online

16.1 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.

17.0 Managing Email

17.1 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.

17.2 The forwarding of any chain messages/emails is not permitted.

17.3 Spam or junk mail will be blocked and reported to the email provider.

17.4 Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

17.5 School email addresses and other official contact details will not be used for setting up personal social media accounts.

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

18 Staff email

18.1 Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

18.2 Members of staff will refer to and adhere to the child protection and safeguarding policy where staff use of mobiles is referred to.

19 Learner email

19.1 Learners will use provided email accounts for educational purposes.

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

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

20 Management of Learning Platforms

20.1 Newnham St Peter's C of E School uses Teams and Seesaw as its official learning platforms.

20.2 Only current members of staff, learners and parents will have access to the learner platforms.

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

20.4 Learners and staff will be advised about acceptable conduct and use when using the learning platforms.

20.5 All users will be mindful of copyright and will only upload appropriate content onto the learning platforms.

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

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

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

20.6.3 Access to the learning platforms for the user may be suspended.

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

20.6.5 A learner's parents/carers may be informed.

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

21 Social Media

21.1 The expectations' regarding safe and responsible use of social media and remote learning platforms applies to all members of Newnham St Peter's C of E Primary School community.

21.2 Members of staff will refer to and adhere to the school's code of conduct and any other policy where the staff use of social media is referred to.

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

21.4 Concerns regarding the online conduct of any member of Newnham St Peter's C of E Primary School'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.

21.5 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.

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

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

21.8 Learners will be advised:

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

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

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

21.8.4 To use safe passwords.

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

21.8.6 How to block and report unwanted communications.

21.8.7 How to report concerns both within the setting and externally.

21.9 Newnham St Peter's C of E Primary School's official social media channels are:
Facebook

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

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

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

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

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

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

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

21.17 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.

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

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

21.20 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.

22.0 Use of Personal Devices and Mobile Phones

22.1 Newnham St Peter's C of E Primary School 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.

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

23.0 Responding to Online Safety Incidents and Concerns

23.1 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.

23.2 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.

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

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

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

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

23.7 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.

23.8 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 Head Teacher / manager

will speak with Gloucestershire Police first to ensure that potential investigations are not compromised.

24 Concerns about Learners Welfare

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

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

24.3 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.

24.4 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

25 Online Sexual Violence and Sexual Harassment between Children

25.1 Our school 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 2021

25.2 Newnham St Peter's C of E Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images including nudes and semi-nudes, and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

25.3 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.

25.4 Newnham St Peter's C of E Primary School recognises 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.

25.5 Newnham St Peter's C of E Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

25.6 Newnham St Peter's C of E Primary School 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 RSE curriculum.

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

25.8 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.

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

25.8.2 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.

25.8.3 Implement appropriate sanctions in accordance with our Behaviour Policy.

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

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

25.8.6 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.

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

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

26.0 Youth Produced Sexual Imagery ("Sexting")

26.1 Newnham St Peter's C of E Primary School 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).

26.2 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".

26.3 Newnham St Peter's C of E Primary School 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.

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

26.5 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.

26.6 We will not:

26.6.1 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.

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

26.6.3 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.

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

- 26.7.1 Act in accordance with our child protection policies and the relevant Gloucestershire Safeguarding Child Board's procedures.
- 26.7.2 Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- 26.7.3 Store the device securely.
- 26.7.4 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.
- 26.7.5 Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- 26.7.6 Inform parents and carers, if appropriate, about the incident and how it is being managed.

26.8 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.

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

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

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

26.12 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.

26.13 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.

27 Online Child Sexual Abuse and Exploitation (including Child Criminal Exploitation)

27.1 Newnham St Peter's C of E Primary School 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.

27.2 Newnham St Peter's C of E Primary School 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.

27.3 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.

27.4 We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.

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

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

27.5.2 If appropriate, store any devices involved securely.

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

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

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

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

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

27.6 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.

27.7 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 the Gloucestershire Police by using 101.

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

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

28 Indecent Images of Children (IIOC)

28.1 Newnham St Peter's C of E Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

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

28.3 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.

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

28.5 If made aware of IIOC, we will:

28.5.1 Act in accordance with our child protection policy and the relevant Gloucestershire Safeguarding Children Partnership Safeguarding procedures.

28.5.2 Store any devices involved securely.

28.5.3 Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Gloucestershire Police or the LADO.

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

28.6.1 Ensure that the DSL (or deputy) is informed.

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

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

28.6.4 Report concerns, as appropriate to parents and carers.

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

28.7.1 Ensure that the DSL (or deputy) is informed.

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

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

28.7.4 Inform Gloucestershire Police via 101 (999 if there is an immediate risk of harm) and Children's Services.

28.7.5 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.

28.7.6 Report concerns, as appropriate to parents and carers.

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

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

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

28.8.3 Quarantine any devices until police advice has been sought.

29 Cyberbullying

29.1 Cyberbullying, along with all other forms of bullying, will not be tolerated at Newnham St Peter's C of E Primary School.

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

30 Online Hate

30.1 Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Newnham St Peter's C of E School and will be responded to in line with existing policies, including anti-bullying and behaviour.

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

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

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

31 Online Radicalisation and Extremism

31.1 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.

31.2 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 Gloucestershire prevent pathway which may include a referral into Channel.

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

32 Cybercrime

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

32.2 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.

32.3 We will make a Cyber Choices referral for early intervention, as per the Cyber Choices toolkit.

32.4 If we are concerned that a child is being exploited as a result of their technical skills, we will follow the Children at Risk of Exploitation (CRE) procedure and the CRE Risk Assessment Toolkit

This policy will be reviewed by governors annually.

Appendix One
Acceptable Use Agreement

Note: All Internet and email activity is subject to monitoring

You must read this agreement in conjunction with the e-Safety Policy. Once you have read and understood both you must sign the acceptance sheet

Internet access – Only children's iPads and laptops are filtered. You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting gender, racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the Head Teacher and an incident sheet completed.

Social networking – is allowed in school in accordance with this e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should think very carefully about making "friends" with parents and never pupils on personal social networks.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act. All school information which contains any data regarding children will only be sent to school email addresses.

Passwords - Staff should keep individual passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pen-drive etc.) is password protected. On no occasion should data concerning personal information be taken off-site on an unsafe device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head Teacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Viruses and other malware - any virus outbreaks are to be reported.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with children.

Mobile Phones – Staff are allowed to carry and mobile phone in school. Phones should not be used for communication or social media throughout the working day unless on school business or during a break. Staff are responsible to ensure that no pupil data, including photographs is on their phone.

Appendix Two

Acceptable Use Charter: Children

Our Charter of Good Online Behaviour

I Promise – to only use the school ICT for work that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I promise – to only use my school email address for school use

I promise- to be ready to learn at home during online lessons (appropriately dressed and following the normal classroom behaviour rules).

I will not – use or share other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – use other people's user-names or passwords.

I will not – share personal information online with anyone and I let my teacher know if anybody asks me for personal information.

I will not – download or upload anything from or to the Internet in school unless my teacher has asked me to.

I will not – install or delete any apps on the school iPads or laptops.

I will not – bring in any electronic device from home (such as a phone, tablet or gaming device). If for any reason I need to for domestic reasons I will hand it to my class teacher at the beginning of the school day.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told

If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to my class teacher or Mrs Nolan.

Name: Signature: Date:

Appendix Three

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
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- 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