Newchurch C.P. School

Preparing To Fly

**Newchurch Community Primary**

**Policy:** Online Safety

**Mission Statement**

Newchurch will give every child a flying start by working in partnership with parents, staff and the community to develop well-rounded citizens who will contribute in a positive way to society.

**Persons with Responsibility**

John Duckett

Lauren Igglesden

Jayne Narraway (Designated Safeguarding Lead)

**Linked Policies**

Computing

Child protection

**Next Review**: September 2023

**Rationale:**

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2022 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside the Newchurch Primary Safeguarding Policy. Any issues and concerns with online safety will always follow the school's safeguarding and child protection procedures.

Online safety encompasses the use of new technologies, internet and electronic communications, such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. Online safety depends on effective practice at a number of levels:

- Responsible use of computing technology by all staff and students; encouraged by education and made explicit through published policies;
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use;
- Safe and secure broadband from Warrington, including the effective management of filtering;
- National Education Network standards and specifications.

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2022).

**Aims:**

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Newchurch Primary School members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

**Roles and responsibilities**

**All staff**

- Read and follow this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education
- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are; notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
- Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- When supporting pupils remotely, be mindful of additional safeguarding considerations.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment as outlined in KCSIE 2022.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues

- Model safe, responsible and professional behaviours in your own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

**Headteacher**

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school).
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how.
- Liaise with the designated safeguarding lead/deputies on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.

**Designated Safeguarding Lead**

- “The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated”
- Work with the HT and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL’s clear overarching responsibility for online safety is not compromised
- Ensure “An effective whole school approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated
- Liaise with the Headteacher and Chair of Governors to ensure that ALL governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and “undertake Prevent awareness training.”
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents.
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.

- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors have asked classroom teachers about this). Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked and why.
- Ensure KCSIE 'Part 5: Sexual Violence & Sexual Harassment' is understood and followed throughout the school and that staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).

**Governors**

- Approve this policy and strategy and subsequently review its effectiveness.
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- "Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach."
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."

**PSHE Lead**

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. “This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils’ lives.”
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress”
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

**Computing Lead**

- As listed in the ‘all staff’ section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

**Network Manager**

- As listed in the ‘all staff’ section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology. Note that KCSIE changes expect a great understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how ‘over blocking’ is avoided as per KCSIE), protections for pupils in the home and remote-learning.

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements

**Data Protection Officer (DPO)**

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document.
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

**Pupils**

- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

**Parents/Carers**

- Talk to the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.

**Reporting and support**

Internal school channels will always be followed first for reporting and support especially in response to incidents, which will be reported in line with the Newchurch Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) referrals to the LA designated officer (LADO).

**Scope:**

This policy applies to all members of the Newchurch Primary School community (including teaching and support staff, supply teachers, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

**Writing and reviewing the online safety policy**

The online safety policy will relate to child protection documents and a variety of curriculum policies. The document will be reviewed regularly by the curriculum leader and other designated staff. This will also happen following any cause for concern or major incident. The governing body will be made aware of any changes to the policy. The policy will reflect the needs and access to communication technologies of the children of Newchurch Primary School. The document will take advice and guidance from Warrington Borough Council, the government, as well as other child and online safety organisations (e.g. NSPCC)

**Teaching and learning:**

**Why Internet use is important:**

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

**Education and curriculum:**

At Newchurch Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework ‘Education for a Connected World – 2020 edition’ from UKCIS (the UK Council for Internet Safety).

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Newchurch Primary will use the Knowsley scheme of work to embed teaching about online safety and harms through a whole school approach, providing an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- Citizenship

It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

“Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.” (KCSIE 2022)

All staff will carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

**Managing internet access information system security**

- School ICT systems capacity and security will be reviewed regularly;
- Virus protection will be updated regularly;
- Security strategies will be discussed with Warrington.

- Newchurch will employ specialist technicians to monitor all onsite systems and to advice on best policy and practise.

**Handling online safety concerns and incidents:**

All staff will be supported in order to recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship). General concerns which relate to online safety will be handled in the same way as any other safeguarding concern.

School procedures for dealing with online-safety will also be linked to the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation

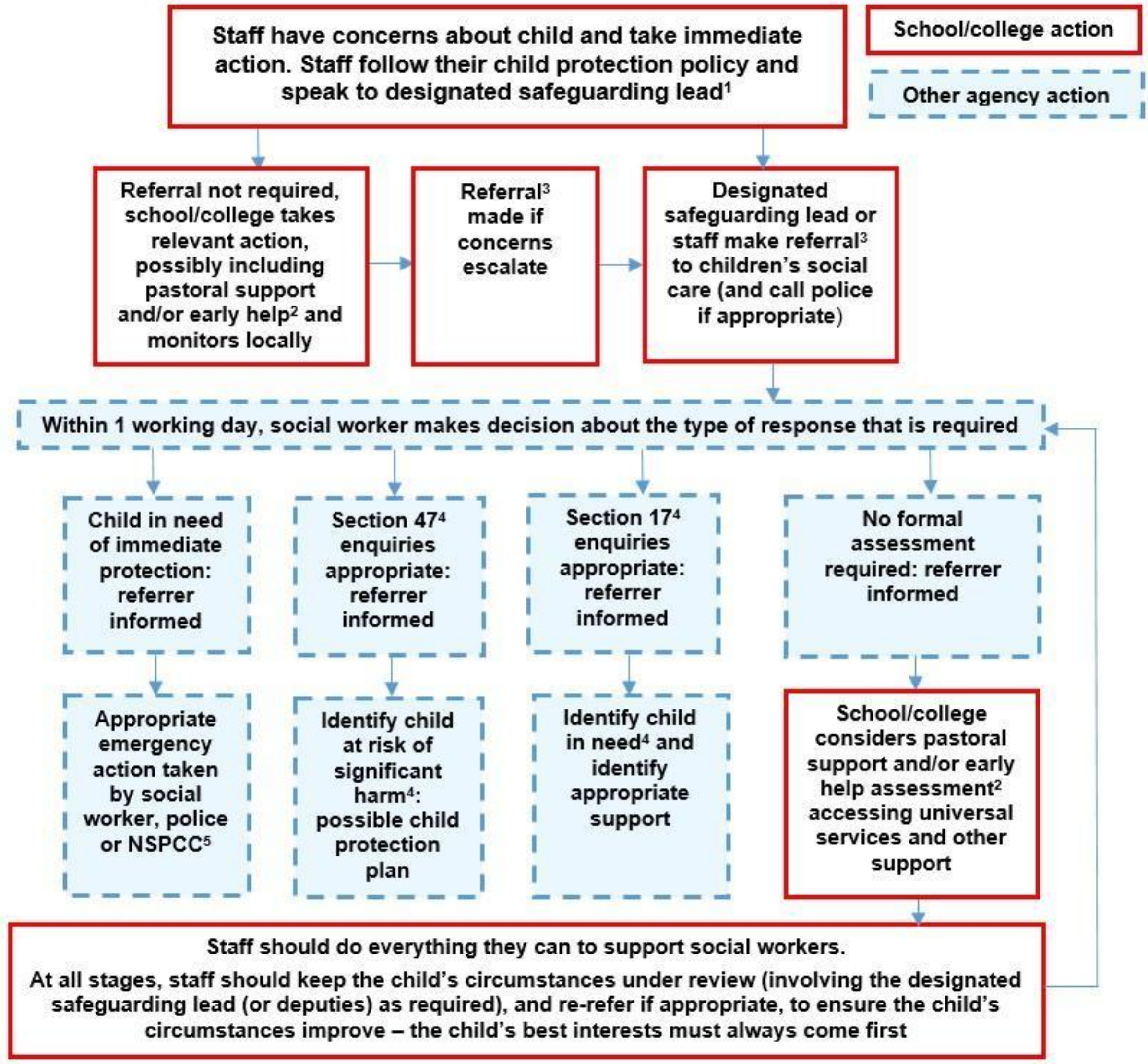
Newchurch Primary School commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline if they have concerns.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). Newchurch will also refer to the DfE guidance 'Behaviour in Schools, advice for headteachers and school staff July 2022' for support in dealing with severe incidents within school.

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting).


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Reportable incidents in school may include (but not be restricted to):

- Sexting – including the sharing of nude images
- Upskirting
- Sexual violence or harassment
- Bullying
- Misuse of technology
- Incidents related to the use of social media

**Data protection and data security**

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children." - 'Data protection: a toolkit for schools' (August 2018)

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The headteacher/principal, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

**Filtering and monitoring**

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At Newchurch Primary School, we have a dedicated and secure connection that is protected with firewalls and multiple layers of security, including a web filtering system, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

School use the Fortinet system for filtering online access. These systems and filters are agreed between Warrington schools and the LA.

The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. School will also work collaboratively with other local schools to establish safer working practices for children and staff.

If staff or pupils discover an unsuitable site, it must be reported to the online safety coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Children will be taught to use the same process at home, keeping communication links open with parents to encourage consistent behaviour at home. Google settings will also be transferred to children logging in on devices beyond school.

**Google Suite for Education**

- All children will be assigned a Google login in under the @newchurchprimary.co.uk domain.
- Children will be given access to a series of recording tools; such as Docs, Sheets, Slides etc.
- The children will also have access to information contained within their class page. This information will be uploaded, managed and reviewed by the staff attached to each cohort.
- The children will be able to interact with work set remotely and return work for feedback. This feedback may be written through Google, recorded through programmes like Kami or given verbally in person.
- Google Classroom will not be a portal for interaction between parents and staff – all parental comments beyond those linked to the completion of a set task will be expected to go through the school office.
- The administration of the Google Suite will be initially established by GBM/Sync before being handed over to Newchurch Primary and technology support (EDAC). The management will be undertaken by the office manager and senior leaders.
- Specific facilities of the Google Suite will be available to all children with others deactivated e.g. gmail.

**E-mail**

- Where email activation is required for any approved curriculum activity, pupils may only use approved e-mail accounts on the school system after written permission from parents. This is unlikely under current Computing curriculum planning.
- The children will be allocated google drive accounts through G-Suite for education. This will be a walled garden ensuring that the children are not receiving or sending emails to external sites.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission. This will be taught explicitly through online safety teaching in each year group;
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- The forwarding of chain letters is not permitted.

**Published content and the school web site**

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published;
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, by checking it regularly. The day to day editorial responsibility will lie with the online safety coordinator and designated staff.

**Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless parental permission has been given;
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs;

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social media feeds;
- Pupil’s work and photographs may be published through the use of the Google Suite or virtual learning environment where group members only have access;
- Children will be taught to use websites outside of the school domain responsibly through online safety teaching;
- Pupil’s work can only be published with the permission of the pupil and parents;
- All permissions linked to the use of, interaction with or publication on school feed and platforms will be gained at the start of each academic year through the data collection process.
- Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.
- All staff are governed by their contract of employment and the school’s Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored.
- At Newchurch Primary School, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices.
- Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.
- Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
- Pupils are taught to think about their online reputation and digital footprint through the computing curriculum.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.
- Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse

**Social networking, personal publishing and social media**

- The school will block/filter access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- Pupils will be advised never to give out personal details of any kind which may identify them or their location;
- Staff will have access to their own class feed in Google Classroom and will be able monitor usage by any member of their cohort. The computing lead, Head and office manager will also be able to monitor individual usage of the Google Suite.
- Pupils and parents will be advised that the use of certain social network spaces, such as Facebook, Instagram, Snapchat, TikTok etc, outside school is inappropriate for primary aged pupils. Parents will be directed towards the www.nationalonlinesafety.com/ site

for additional guidance on current online risks and advances, including those linked to gaming and social media;

- Children will be taught how to use social network sites safely through the curriculum and My Online Life units in each year group;
- Where necessary, guidance videos will be made for parents to model the safe and accurate use of school-based resources and programmes.
- Newchurch Primary School's social media platforms will be managed by staff and content reviewed by the senior leadership team. The Facebook account will be entirely managed by the headteacher and the Twitter feed by all designated staff.
- Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.
- This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.
- If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).
- Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school does deal with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.
- School has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse.
- Email is the official electronic communication channel between parents and the school, and between staff and pupils.
- Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.
- Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

  * Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).

  ** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

- Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

**Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed;
- Mobile phones will not be used during lessons or formal school time – this includes on school trips and residential visits. The sending of abusive or inappropriate text messages is forbidden;
- Staff will use a school phone or school approved programme which records all calls as having being sent by school where contact with pupils is required.
- Guidance will be suggested to parents through online professionals (e.g https://info.nationalonlinesafety.com/mobile-app)

**Assessing risks**

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor WBC can accept liability for the material accessed, or any consequences of internet access;
- The school will audit computing provision to establish if the online safety policy is adequate and that its implementation is effective.

**Handling Online safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff;
- Any complaint about staff misuse must be referred to the Headteacher;
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and reported to the Designated Senior Leader (DSL) and recorded on the confidential CPOMS service;
- Pupils and parents will be informed of the complaints procedure;
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

**Safeguarding against radicalisation, extremism and terrorism**

- Staff trained through 'Prevent' initiative.
- Children's internet use monitored during sessions.
- E-mail facilities disabled on all pupil Google-based accounts.
- Children educated about the risks of meeting people met online.
- Children made aware of the dangers of radicalisation at appropriate points without indoctrination to any belief offering balanced view – in line with government Prevent guidance.

- Other safeguarding methods named in this document will be in place e.g. filtering and awareness.
- Staff made aware of places to seek advice on safe internet use e.g. https://www.saferinternet.org.uk/ and https://info.nationalonlinesafety.com/mobile-app
- British values programme taught through PSHE to ensure children are aware of diversity within British culture without indoctrination.

**Community use of the Internet**

- External organisations using the school's computing facilities must adhere to the online safety policy.
- In line with the communication policy, safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year;
- Pupils will be informed that network and Internet use will be monitored.
- Staff and the Online safety policy
    - All staff will be given the School Online Safety policy and its importance explained;
    - Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
    - Staff induction will support the training of staff in these practices and will also be applied to visiting staff e.g. student teachers.

**Enlisting parents'/carers' support**

- Parents'/carers' attention will be drawn to the School Online Safety policy through workshops, in newsletters, school social media feeds and through documentation on the school Web site;
- Parents will be directed towards professional and up-to-date guidance in order to help keep their children safe e.g. https://info.nationalonlinesafety.com/mobile-app

**School website**

- The Headteacher/Principal and Governors have delegated the day-to-day responsibility of updating the content of the website to the school administrative staff and senior leaders. The site is managed by / hosted by eschools.
- The website will hold key information for parents and carers, statutory documents and images of school life, including children whose parents/carers have given express permission. Full names and personal information will not be published online.

**Why might the internet or communications technology be used?**

| Activities | Key online safety issues | Relevant sites and programmes |
|---|---|---|
| Using search engines to access information from a range of websites. | Pupils should be supervised.<br>Pupils should be taught what internet use is acceptable and what to do if they access | Kidrex.org |

| | | |
|---|---|---|
| | material they are uncomfortable with. | |
| Exchanging information with other pupils and asking questions of experts via e-mail | Pupils should only use approved email accounts. Pupils should never give out personal information. | Google Suite for education |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication. Child names should be omitted if using websites outside of school-based programmes. | Google Suite for Education<br>School social media feeds |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought. File names should not refer to the pupil by name. | Google Suite for Education<br>School social media feeds |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised. | Google Meet |