THE FEDERATION OF NETTLESTONE & NEWCHURCH PRIMARY SCHOOLS

E-SAFETY POLICY

Date Agreed: Nov 2021

Review Date: Nov 2023

Signed: _____
Co-Chair Board of Governors

Signed: _____
Executive Headteacher

Revision No.	Date Issued	Prepared By	Approved	Comments	Policy owned by LR
1	November 2014	VH		Small amendments in light of Federation	
2	November 2015	AT		Minor additions, mostly around social media	
3	November 2016	AT		Addition of E-safety in the curriculum criteria	
4	April 2019	LR		Annual update	
5	April 2020	AT		Annual Update	
6	April 2021	LR		Annual Update. Small amendments in light of discussion with the Nettlestone Cyber Ambassadors (definition of plagiarism and the importance of safe searching when researching online).	
7	November 2021	LR/KI		Development, monitoring and review of the policy. Removal of Cyber Ambassadors as due to COVID-19 training has not occurred remotely with new cohort of ambassadors for academic year 21-22. Amendment to the E-safety curriculum included (use of the Project Evolve Framework). Signpost to Computing section of each school's website to find the 'I can' statements to support the delivery and content of the E-safety/digital literacy of the Computing Curriculum. Removal of E-safety skills 'I can' table as a result. Addition of Lurking Trolls Campaign Launch and how this campaign supplements our E-safety/digital literacy curriculum across the Federation. In 'Use of digital images' section, the reference to 'Vine' has been removed due to the shutting down of this platform. Instead, this has been replaced with reference to TikTok as there is exposure to this currently within our school community (particularly UKS2 pupils).	

All the governors and staff of The Federation of Nettlestone & Newchurch Primary Schools are committed to sharing a common objective to help keep the children and staff of the school community safe. We ensure that consistent effective safeguarding procedures are in place in order to support families, children and staff of the school.

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of contexts to promote effective learning.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the child or young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-safety policy is used in conjunction with the school's Positive Behaviour, Anti-bullying and Child Protection policies. As with all other risks, it is impossible to eliminate risks completely. It is therefore essential to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. This E-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help children (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development, monitoring and review of this policy

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Full Governing Body and Leadership and Management Committee meetings
- School website and newsletter.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys/questionnaires of pupils, parents/carers and staff.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers Executive Headteacher/Head of School, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this and associated policies and will, where known, inform parents/carers of incidents of inappropriate E-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Leadership and Management Sub Committee receiving regular information about E-safety incidents and monitoring reports.

Executive Headteacher/Head of School and Senior Leaders:

- The Executive Headteacher/Head of School is responsible for ensuring the safety (including E-safety) of members of the school community, though the day to day responsibility for E-safety will be delegated to the Computing Lead.
- The Head of School is responsible for ensuring that relevant staff receive suitable Continuing Professional Development (CPD) to enable them to carry out their E-safety roles and to train other colleagues, as relevant.
- The Head of School will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role.
- The Executive Headteacher, Head of School and middle leaders should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.

Computing Lead:

- takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments
- attends relevant staff and Leadership and Management Sub Committee meetings
- reports regularly to the Executive Headteacher/Head of School.

The ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- that the school meets the E-safety technical requirements outlined by any relevant Local Authority E-safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant
- that the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Executive Headteacher/Head of School/ICT Leader for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current school E-safety policy and practices
- they have read, understood and signed the school staff Acceptable Use Policy
- they report any suspected misuse or problem to the Head of School/ICT Leader for investigation/action/sanction
- digital communications with pupils should be on a professional level and, where possible, carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school E-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection

should be trained in E-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying.

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy which parents/carers will be expected to sign on behalf of pupils before they are given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism (copying of another's work without acknowledgement) and uphold copyright regulations.

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying
- should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand potential issues through newsletters, letters, the school website/Facebook page and information about national/local E-safety campaigns and presentations/courses. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

E-safety education will be provided in the following ways:

- A planned E-safety programme will be provided as part of ICT/Personal Health Social Economic (PSHE)/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. The Federation of Nettlestone and Newchurch have chosen to adopt the Project Evolve Framework. Further information regarding this framework and the 'I can' statements for each year group can be found under the Computing section of each school's website
- Alongside the Project Evolve Framework, the Lurking Trolls campaign has been launched (November 2021). The campaign is backed by the Safeguarding Children Partnerships in Portsmouth, Southampton, Isle of Wight and Hampshire and is designed to educate and protect children from online harm. In addition, the aim of the campaign is to build digital resilience. This means our children will be able to:
    - Understand there are some risks online, and that these come in different forms
    - Know where to turn for help when they encounter risks, or when something difficult or unpleasant happens
    - Can learn and recover from their experiences. (Source: https://lurkingtrolls.com/parents/)
- Key E-safety messages will also be reinforced as part of a planned programme of assemblies
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils will be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education & Training – Staff

It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- This E-safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The Computing Lead will provide advice/guidance /training as required to individuals as required
- All new staff will receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Policies.

Training – Governors

Governors should take part in E-safety training/awareness sessions, with particular importance for those who are members of any sub-committee involved in ICT/E-safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities.
- School ICT systems will be managed in ways that ensure that the school meets the E-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. Users will be required to change their password regularly.
- The "administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Executive Headteacher/Head of School and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Internet access in the school is provided via a broadband link which is filtered by RM SafetyNet Plus, who block access to any material they do not feel is appropriate.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Executive Headteacher/Head of School (or other nominated senior leader).
- Any filtering issues should be reported immediately by the Network Manager to RM.

- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Executive Headteacher/Head of School. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the ICT Leader.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual/potential E-safety incident to the ICT Leader or Executive Headteacher/Head of School.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/ DVDs) by users on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

- E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages in the use of ICT across the curriculum.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. social networking, Facebook, X-Box Live, messaging – SnapChat, Instagram, TikTok, WhatsApp etc.

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, 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 (as part of the Acceptable Use Policy signed by parents or carers at the start of the year).

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communications technologies

Mobile Phones

The use of mobile phones will not be permitted during lessons or formal school time by staff or pupils. This excludes occasions when staff may need to use mobile phones, for example on school trips, or as part of a

demonstration in a lesson. Staff may use their mobile phones in the staff room outside of formal school time but they must be switched off/on silent and not used for personal reasons during the time staff are with children.

School Website

The school website is maintained and kept up to date by the Head of School, the IT Technician and administration staff. The Head of School ensures that the content on the school website is accurate and appropriate to the needs of the school community. No personal information about any member of the school community will be published on the website.

Social Networking

The use of public online chat rooms, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the E-safety of the pupils. Thus, public social networking sites and newsgroups will be blocked and filtered. Pupils are advised never to give out any personal details that might identify them or their location. Pupils are advised not to place personal photos on any social network space. Pupils are advised on security and encouraged to set passwords and deny access to unknown individuals. Pupils are advised never to agree to meet someone they have met on a social networking site. Should pupils have any concerns about social networking sites or chat rooms, they are advised that they must tell a trusted adult.

Staff must not publish children's surnames on school social media sites. Only children whose parents have given specific written consent may be posted on school social media sites. When posting on social media sites such as Facebook, staff must not give details of exact locations where children can be found for events outside of usual school days and times.

Email

- Curriculum activities that involve the use of email will be delivered through email programmes that are controlled by the school and only use email accounts that are approved by the school.
- The use of individual pupil personal accounts will not be permitted through the school system.
- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Responding to incidents of misuse

All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school E-safety policy. It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be

times when infringements of the policy could take place through careless, irresponsible or, very rarely, deliberate misuse. The Executive Headteacher/Head of School will ensure that the E-safety policy is implemented and compliance with the policy monitored. If members of staff suspect that misuse might have taken place, they should be referred to the Executive Headteacher/Head of School. It is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.