Phoenix Integrated Primary School.

ICT / Online Safety / Acceptable Use of Internet and Digital Technologies Policy

Policy Developed: 12.11.14

Updated /Reviewed: T1 2023/24

Review by Governors:

Signed:

Phoenix Integrated Primary School ICT Vision.

We believe in the holistic development of the child to his/her potential. It will provide a broad, balanced and differentiated curriculum.
At Phoenix Integrated Primary School our vision is to create motivated 'life-long' learners through the use of ICT to enhance and extend learning and teaching across the whole curriculum. As ICT is continually developing and new technologies emerging, we as a school will strive to give all pupils the skills to prepare them for a future in which ICT is an integral part of society.

Our vision encompasses the following aims:

- ICT will be embedded into every day school life by enabling pupils to explore express, exchange, evaluate and exhibit their work.
- To provide opportunities to enable all our staff, pupils and parents to be confident, competent and independent users of ICT.
- To provide an environment where access to ICT resources is natural and commonplace.
- To ensure ICT has a fundamental role in developing and enhancing our school's key learning aims in promoting the pupils' educational, physical and social needs.
- To use ICT to develop an online community, sharing ideas and resources between pupils, staff, parents, Board of Governors, other schools and the wider community.

Development of this Policy.
Consultation of the whole school community has taken place through the following.

- Staff meetings.
- Children Questionnaires.
- Governor Questionnaires.
- Parent Questionnaires.

The consultation process has included guidance from individuals and documents from the following outside agencies:

- Department of Education – eSafety Guidance 2013/25.
- C2K.
- South West Grid For Learning (SWGFL) – 360 Online Safety self review tool.
- Microsoft Partners in Learning.

Introduction.
Information and Communications Technology (ICT) is changing the lives of everyone. ICT is a generic term used to denote the convergence of computers, video and telecommunications, as seen in the use of multi-media computers, mobile phones, gaming consoles etc.

We aim to enable our pupils to find, explore, analyse, exchange and present information. We also focus on developing the skills necessary for children to be able to use information in a discriminating and effective way.

Phoenix Integrated Primary School meets the requirements set out within the Northern Ireland Curriculum and develops the use of the 5Es within the tasks already being carried out through:

- Explore.
- Express.
- Exchange.
- Evaluate.
- Exhibit.

ICT forms part of the School Development Plan and is reviewed annually.

Phoenix Integrated Primary School is well equipped with networked laptops and PCs in each class. The school also has 79 Apple iPads.

Every class has access to:

- A class desktop.
- Networked laptops
- A digital camera
- An Interactive Whiteboard
- Use of a class set of iPads
- Beebots/probots/roamers/mats
- Webcam/ Hue Camera

Strategies for use of ICT.

- ICT is not taught as a distinct subject, but it is a tool to be used as appropriate throughout the curriculum.
- All pupils are given equal access.
- ICT is an entitlement for all pupils.
- Common tasks are set that are open-ended and can have a variety of responses.
- We provide suitable learning opportunities for all children by matching the challenge of the task to the ability and experience of the child.
- Use of ICT at home will continue to be encouraged through projects, homework and the use of My School which can be researched through a home computer system or at the local library.

ICT Competences.
At Phoenix Integrated Primary School we endeavour to help our pupils to develop competence in the use of ICT.
ICT competence is concerned with:

- Learning about ICT – developing the knowledge and skills required to use ICT effectively and to apply these in a range of contexts.
- Learning through ICT – developing the skills required to access and use information from a range of electronic sources, interpret it and use it effectively.
- Learning with ICT – applying the skills in their own learning either at school, at home or in the community.

ICT and the Northern Ireland Curriculum.

Literacy.

- ICT is a major contributor to the teaching of Literacy.
- Children learn how to draft, edit and revise text.
- Children can create, develop present and publish ideas and opinions visually or orally.
- They learn how to improve the presentation of their work by using desk- top publishing and presentational software.

Numeracy.

- Many ICT activities build upon the mathematical skills of the children.
- Children use ICT in Numeracy to collect data, make predictions, analyse results, and present information graphically.
- They can explore mathematical models e.g. use of BeeBots, Probots and spreadsheets.

Personal Development and Mutual Understanding (PDMU)

- ICT makes a contribution to the teaching of PDMU and citizenship as children learn to work together in a collaborative manner.
- They develop a sense of global citizenship by using the Internet.
- Through the discussion of moral issues related to electronic communication, children develop a view about the use and misuse of ICT as exemplified through the use of My School.
- They also gain a knowledge and understanding of the interdependence of people around the world.

Creative and Expressive.

- ICT offers children the freedom to express their own ideas creatively and to experience the designs of others.
- Children will have the opportunity to develop their creativity through a range of network software and digital technology.

- They can explore the Internet to gain access to a wealth of images and information about world famous pieces.

World Around Us.

- ICT transcends the barriers of distance and opens up the world as an easily accessible global community allowing children to experience the past, present and future of the world they live in.

Inclusion.

Phoenix Integrated Primary School's ICT facilities are available for use by all pupils and staff. All children are given access to ICT regardless of gender, race, physical or sensory disability. ICT can impact on the quality of work that children can produce and it can increase their confidence and motivation.

The Special Needs team have access to networked laptops and iPads to support their everyday teaching and learning strategies.

Progression, Monitoring, Assessing and Evaluating.

Progression.

- All children develop and learn at their own pace.
- Each class teacher ensures that children attain skills from a class ICT skills checklist, found in each pupil's file.
- Progression is assured through a range of increasingly challenging activities covering all areas of ICT and embedded in the Northern Ireland Curriculum. Foundation Stage – 3 tasks developed within each year group within existing curricular areas.
- Key Stage 1 and Key Stage 2 – 3 tasks from the CCEA Using ICT Cross Curricular Skills Tasks are assigned appropriately throughout the year groups.

Monitoring.

- Evidence covering all areas of ICT is garnered within each pupil's folder.
- It is currently the responsibility of the ICT team to monitor the standard and progress made by each pupil by gathering appropriate evidence termly during each school year. This is in preparation for the statutory assessment of Using ICT by every teacher from P3-P7.

Assessing.

- Evidence gathered each year is assessed by the ICT Co-ordinator and the ICT team. Evidence may also be submitted to CCEA as part of moderation within the Using ICT Cross Curricular Skills.

Evaluating.

- Evidence gathered each year is summarised within a self-evaluative report.

ICT Co-ordinator.

- It is the responsibility of the ICT co-ordinator to assist all teachers with the implementation of this policy.
- The ICT co-ordinator has the responsibility for the management of the resources, which are required for the implementation of this policy.
- The ICT team will disseminate information regarding new developments in ICT to other members of staff.
- The ICT team will be responsible for any staff INSET in the development of ICT.
- It will be the responsibility of the ICT co-ordinator to ensure that the system for reviewing this policy is initiated.
- The ICT Co-ordinators will be responsible for the updating of policy, action plans and Internet guidelines and informing staff of aforementioned documents.
- The ICT Co-ordinator will have implemented a maintenance log system and liaise with C2K/Capita in the maintenance of the hardware and software within the school.
- The school and ICT team will promote and provide organised CPD to staff to help ensure they are kept abreast of any emerging technologies.

E Safety Policy / Acceptable use of the Internet and Digital Technologies.

(See also Social Media Policy)

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. The 'MySchool' and 'Fronter' services will present many opportunities for all pupils. It will give teachers and pupils access to learning resources from across the world and will bring these resources into the classroom. Access to the internet and its resources will be possible from any internet connected device, 24 hours a day. This allows teachers, pupils and parents to work in partnership to support learning. The communications and e-learning elements of the service will support collaboration between schools and will offer pupils a richer learning experience. Children and young people have an entitlement to safe internet access at all times.

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

Governors: Roles and Responsibilities

Governors are responsible for the approval of the ICT / Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about Online Safety incidents and monitoring reports. The role of the Online Safety Governor will include:

- Regular meetings with the ICT coordinator.
- Regular monitoring of Online Safety incident logs

- Reporting to relevant Governors committee / meeting

Principal and Senior Leaders:

- The Principal and Governors are responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the ICT team.
- The Principal / Senior Leaders are responsible for ensuring that the ICT Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Principal/ Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. (This is to provide a safety net and also support to those colleagues who take on important monitoring roles.)
- The Principal and one member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed and monitored by C2k/Northgate.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- They will report any suspected misuse or problem to the ICT Co-ordinator or Principal for investigation.
- Digital communications with pupils (email / Virtual Learning Environment (VLE) or voice) should be on a professional level.

The following is a breakdown of the privileges each member of staff will hold when accessing the internet through the C2K system. Note: This is only when logged on to a computer or laptop. Normal internet filtering will continue on iPads to ensure children are able to safely use the internet.

Principal: Internet Social Networking- overseeing use by staff
Internet Streaming Media.
Internet Advanced.

Teaching staff: Internet Streaming Media.
Internet Social Networking.
Internet Advanced.

Non teaching staff: Internet Advanced.

There are certain dangers. It is the class teacher's responsibility to ensure that any content used in class is thoroughly checked before used in the classroom.

Also, when using Youtube, it is advised to turn off the IWB when searching for a particular video. Turn it on to play the video. As soon as the video is over, turn the whiteboard off and shut down Youtube. There are opportunities for inappropriate images to flash up in Youtube, even if the material has been checked.

Internet Connection (October 2018)

Service Provided by C2k- Filtering on the C2K Network.

The school has recently opened up the access privileges for internet connection, 'C2K Wireless.' Each iPad can now be set up using a unique code with keeps each iPad connected to the school network. Although this provides for better connectivity and reduces hassle of connecting more than once, it does allow pupils to access the network more freely. Teachers will need to monitor much more closely iPad use during this time, especially during any independent or paired work. Using apps such as 'Kids YouTube' will provide for much safer use.

Designated person for child protection / Deputy designated Child Protection Officer:

Will be trained in Online 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

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 help parents to understand these complex issues. Parents also have a duty to use social media, linked with the school, in a responsible manner (see guidance in social media policy) Parents and carers will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy.

Appointed Governor for Safeguarding.

Shauna Mulligan has been listed as Goversnor for Safeguarding as of 13.03.18

Education

Pupils:

Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy and Social Media Policy, which they will be expected to sign along with their parents before being given access to school systems.

Online Safety education will be provided in the following ways:

- A planned Online Safety programme should be provided as part of PDMU lessons, assemblies, School Council meetings. This will cover both the use of ICT and new technologies in school and outside school.
- The school mark Internet Safety week and pupils enter associated events such as Safer Internet Day Organised by EA/C2K
- Pupils are made aware of how to report a problem i.e. initial report to class teacher who thens passes onto Mr Crooks (ICT Coordinator) or Mrs Watson (Principal). A record is kept of potential breaches of online safety. This is maintained in the ICT coordinators classroom.
- Pupils are not permitted to carry or have possession of mobile phones while at school.

Education of parents and wider community:

- The school will from time to time provide information and training for parents where appropriate- workshops/ talks

Education & Training – Staff.

- All staff will be kept up to date with e- safety policy training and developments.
- It is agreed that all staff- teachers, sub teachers, students and guests will use the ICT systems in a professional and responsible way.
- All teachers have received CEOP training and become accredited CEOP facilitators.
- Internet safety is included as part of Safeguarding and Child Proctection training.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum. Pupils will be guided to suitable sites by their teacher.

Use of Digital Images - Photographic, Video.

- Video and digital images are only to be used with the person's permission. They are to be used for educational purposes only.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, using, sharing, publishing and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet.
- The Use of Digital Images / Photograph / Video Permission document is to be signed by parents and kept in the pupil file. The document is attached at the end of this policy.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored by C2K**.** Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications will be monitored
- Users must report immediately to nominated person, the receipt of any e-mail that makes them feel uncomfortable or is offensive, threatening or bullying in nature. They must not respond to any such email.
- Any digital communication between staff and pupils or parents (email, chat, VLE etc) must be professional in tone and content.

Responding to incidents of misuse

If any misuse is observed, it should be reported to a teacher, who will then report to a member of the safeguarding team by a teacher. The principal may wish to inform the Governors or other related outside agencies - social services, SELB, Police. These incidents will be logged in the Online Safety Incident Log kept in coordinators classroom.

In cases of pupil misuse, pupils will have internet access removed for a specified period of time.

Other sanctions may apply depending on the incident and be in line with the school's Behaviour Policy.

Guidelines for a Code of Conduct for those who work with children and young people.

Social networking is everywhere. It is common to find parents, children, co - workers and others on such sites. With social networks people across the world have access to

tools and options that were previously non - existent. However, there are now just as many new opportunities to connect as there are to get into potential danger. One thing we often forget while having fun on social networks is that almost anybody can see what we are doing. While we are tagging photos for our friends or are posting comments to them, it can be easy to forget that someone else who has been invited onto a social networking site can also view them.
Once something appears on the Internet, it's almost impossible to remove. As these sites continue to grow in popularity, so too does the value of the information on them to parties other than those directly involved. Social networking users need to take a step back and think about just what they're posting onto the Internet.

Guidelines.
People who work with children and young people should always maintain appropriate professional boundaries, avoid improper contact or relationships and respect their position of trust.

With regard to relationships, individuals who work with children and young people should not attempt to establish an inappropriate relationship which might include:

- Communication of a personal nature.
- Inappropriate dialogue through the internet.
- The sending of emails or text messages of an inappropriate nature.
- It is advisable that teaching and non-teaching staff do not add parents/carers of pupils in this school as friends of social media. If staff have a links with parents/carers on social media, they do so at their own risk. (However, we are aware that in some instances members of staff may be related to or have prior friendships with parent/carers.)
- Staff should never discuss school business in a negative manner.

Individuals, who work with children and young people, should be extremely careful in corresponding with people on social networking sites. Staff relationships with children and young people should at all times remain professional and they should not correspond with children and young people through such sites or add them as 'friends'. It is worth bearing in mind that on such sites an inappropriate or even misconstrued communication may have the potential to impact upon their careers or even result in criminal investigation. In addition staff should bear in mind who may access their own profiles on such websites and should therefore take care as to the information they display about themselves and their personal lives. They should also ensure that they have installed and are using the appropriate privacy settings.

Individuals who work with children and young people, should not make, view or access illegal or inappropriate images of children.
Individuals who work with children and young people and others, with whom they may be in a position of trust, should exercise caution when using social networking sites and avoid inappropriate communication of any kind.

Coronavirus Pandemic

Appendix 1 outlines the schools' procedures that have been put in place to ensure safeguarding of pupils during the Coronavirus pandemic (since 23rd March 2020). This section will be updated as and when required in accordance with new guidance.

This policy, in line with Department of Education Guidelines, should be reviewed annually.

Date on which policy was approved:

Phoenix Integrated Primary School – Pupil Acceptable Use Policy.

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child): _____

Phoenix Integrated Primary School - Staff Acceptable Use Policy Agreement.

School Policy
New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement.
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:
- I understand that the School Leadership Team will monitor my use of the ICT systems, email and other digital communications.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name: _____

Signed: _____ Date: _____

Appendix 1
Arrangements for remote learning during Covid-19 *(updated May 2020)*

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social services as required.

Online teaching should follow the same principles as set out in the school's code of conduct. Phoenix Integrated Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. During the period of school closures, pupils across the school have taken part in various forms of remote learning through apps, websites and services offered by C2K. How to access these mediums has been shared with pupils and parents through letters, social media posts and text messages.

Online Teaching Tools

Below is a breakdown of what each class is using as their main teaching and learning tool. All the listed platforms comply with GDPR and data protection. Information shared by the class teacher over the platforms is only to do with teaching and learning.

Year1- Seesaw
Year 2- Seesaw and Mathletics
Year 3- Seesaw
Year 4- Study Ladder and Mathletics
Year 5- Study Ladder and Google Classroom
Year 6- Google classroom
Year 7- Google classroom

Through our social media pages, parents and pupils have been able to access age appropriate online safety advice and resources. Pupils using Google classroom have been reminded of how to suitably communicate with their peers. Pupils are 'muted' when the class teacher is not there to monitor comments, over periods such as weekends, Bank Holidays etc.

Delivering Virtual Lessons

Below are some measures our staff consider when assigning or delivering virtual lessons.

- Teaching should take place during the normal hours of a school day
- No 1:1s, groups only
- If tutorials or lessons are recorded, staff must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- Language must be professional and appropriate, including any family members in the background.

- Staff must only use platforms approved by the ICT team and following C2K advice

Teachers' contact details

All teachers have set up a Gmail e-mail address so that parents can communicate with them while they are working from home. Staff are made aware that this e-mail account is only to be used for school use and to communicate with the parent about their child's learning. To protect the teachers' professional privacy, it was agreed that they would not give out their c2k e-mail addresses.

Appendix 2

Arrangements for returning to school *(Updated August 2020)*

Phoenix Integrated Primary School will continue to ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. As the school continue to use online platforms for extending and consolidating teaching and learning, pupils across the school will continue to take part in various forms of remote learning through apps, websites and services offered by C2K. How to access these mediums has been shared with pupils and parents through letters, social media posts and text messages.

Online Safety

Reminders of being safe online will be shared with pupils upon return to school.

Risks online

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

- The school continues to ensure appropriate filters and monitors are in place
- Our governing body will review arrangements to ensure they remain appropriate
- The school has taken on board guidance from the UK Safer Internet Centre on safe remote learning and guidance for safer working practice from the Safer Recruitment Consortium. We have reviewed the code of conduct and information sharing policy accordingly.
- Staff have discussed the risk that professional boundaries could slip during this exceptional period and been reminded of the school's code of conduct and importance of using school systems to communicate with children and their families.
- Children and young people accessing remote learning receive guidance on keeping safe online and know how to raise concerns with the school, Childline, the UK Safer Internet Centre and CEOP.
- Parents and carers have received information about keeping children safe online with peers, the school, other education offers they may access and the wider internet community. We have set out the school's approach, including the sites children will have asked to access and set out who from the school (if anyone) their child is going to be interacting with online. Over the coming weeks, parents will be offered the following links:
    - Internet matters - for support for parents and carers to keep their children safe online
    - Net-aware - for support for parents and careers from the NSPCC
    - Parent info - for support for parents and carers to keep their children safe online

- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers

Loaning Device Requests

The school are in a position to lend devices to vulnerable and disadvantaged pupils. This loaning of devices was offered to families during the period of school closure (April-June 2020) Vulnerable pupils are identified by their class teacher and parents can be offered a device or devices depending on their needs. Devices are signed out of school using a record sheet and signed back into school when the need returned (see appendix 3)

More devices can be requested through the Education Authority. M Crooks can fill out a form to request a device. Below are the priority criteria outlined by the education minister for the loaning of devices:

1. Priority will be given to children in year groups: 11, 13, 6 and 3; and
2. Categories: FSME, SEN 1-5, Newcomer target groups (this means Asylum Seeker, Refugee and Roma children), LAC and children who are considered vulnerable.
3. Distribution of devices shall be given in the following priority order:

    A. Current Year 11 pupils who are FSME and SEN or newcomer target groups or LAC or vulnerable;
    B. Current Year 13 pupils who are FSME and SEN or newcomer target groups or LAC or vulnerable;
    C. Current Year 6 pupils who are FSME and SEN or newcomer target groups or LAC or vulnerable;
    D. Current Year 3 pupils who are FSME and SEN or newcomer target groups or LAC or vulnerable;

Password Retrieval:

It is important that pupils are reminded of the importance of password privacy. **However, there may be instances where passwords need to be changed or have been forgotten. Below are the steps to follow if this is the case.**

For school staff:

If a staff member's password expires and they don't remember their password, in the first instance they should contact a C2k manager in their school who will be able to reset their password for them. If they are unable to contact their school, please contact the C2k Service Desk.

For pupils:

If a pupil's password expires and they don't remember their password, in the first instance they should contact a technician or teacher in their school. They will be able to reset the pupil's password for them.

In circumstances where they are unable to contact their school, please ask a parent or guardian to email resetmypassword@c2kni.org.uk and provide the following information:

- Student First Name and Surname
- Student Date of Birth
- Student Username
- Name of School
- School Address

When EA staff make contact, the parent/guardian will be asked to provide some other details to verify the pupil's identity: The member of C2k staff will check the details provided against the records held in the school and once verified, will reset the pupil's password.

Acceptable use and code of conduct

Staff

Staff will be reminded of their code of conduct when interacting with pupils through learning platforms.

Pupils

The procedures for dealing with any inappropriate online behaviour will remain in place (see page 11-12 of ICT Policy) As pupils will be spending more time online, they will be reminded of the rules and expectations.