Ballykeel Primary School & Nursery Unit

Online Safety & Acceptable Use of the Internet and Digital Technologies Policies

Reviewed September 2023

Acceptable Use of The Internet and Digital Technologies Policy

This policy is based upon the following DENI Circulars: 2016/27 on Online Safety, 2013/25 on e-Safety Guidance, 2011/2 on Internet Safety and 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools, and operates in conjunction with Ballykeel Primary School's Online Safety Policy

1. Introduction

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."
(DENI Curricular 2007/1)

In Ballykeel Primary School and Nursery Unit we recognise that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform learning and teaching when used effectively and appropriately. In the 21st Century the Internet is an essential resource for education, business and social interaction.

Ballykeel PS & NU provides opportunities for pupils to use the Internet, along with helping them develop the skills necessary to access, analyse and evaluate resources available online. This includes educating our children about the potential dangers found on the Internet, and our Online Safety Policy further explains our role in protecting our pupils.

2. Code of Practice for Safe and Effective Use

When using the Internet, email systems and digital technologies, all users must comply with relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The Code of Practice for Ballykeel PS & NU sets out for all users, staff and pupils, what is safe and acceptable and what is not.

The scope of the Code of Practice covers fixed and mobile Internet, school desktop computers, laptops, iPads and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought onto school premises or taken on trips (e.g. mobile phones, camera phones, iPads etc.) is subject to the same requirements as technology provided by the school.

The ICT Co-ordinators will monitor the effectiveness of the Code of Practice, particularly in light of new developments in technology.

2.1 Code of Practice for Pupils

Pupil access to the Internet is through a filtered service provided by C2k, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents before pupils access the Internet.

In addition, the following measures have been adopted by Ballykeel PS & NU to ensure our pupils do not access any inappropriate material:

- Our Online Safety rules (*Appendices 1A & 1B*) and advice for staying 'SMART' online (*Appendix 2*) are delivered to pupils, accessible on our school website, and displayed prominently in the ICT Room/classrooms;
- We review regularly Our Code of Practice (Rules for Using Computers/iPads in School - *Appendix 3)* which is signed by pupils/parents when pupils entering P1 and P4, and when joining the school for the first time (*Appendices 4A & 4B)*;
- Pupils using the Internet will be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised, where possible;
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group, unless engaging in independent research activities;
- Pupils are not permitted to download apps onto school iPads (with the exceptional of Digital Leaders, under teacher supervision);
- Pupils are educated in the safe and effective use of the Internet, through lessons provided by Safer Schools NI and teacher led activities during Safer Internet Week.
- An Online Safety Team has been established, consisting of the two ICT Co-ordinators and the Designated Teacher for Child Protection. The team will review any Online Safety issues that arise, and monitor any concerns raised by a pupil, or the safeguarding tool Securus Education (see Online Safety Policy Point 8 for further information about Securus).

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2k can accept liability under such circumstances.

The use of mobile phones by pupils is not permitted on the school premises during school hours, or on school trips.

Pupil access to social networking sites is blocked by the C2k filters so pupils do not have access to them in the school environment. During school hours pupils are forbidden to play computer games unless specifically assigned by the teacher.

2.2 Sanctions

Incidents of technology misuse which arise within school will be dealt with in accordance with the school's Positive Behaviour policy. Minor incidents will be dealt with by the Online Safety Team and may result in a temporary or permanent ban on Internet use. Incidents involving Child Protection issues will be dealt with in accordance with school Child Protection procedures. Incidents involving the use of social media with regard to the school, pupils, parents or members of staff may be dealt with in accordance with our Social Media Policy.

2.3 Code of Practice for staff

Staff have agreed to the following Code of Safe Practice:

- Pupils accessing the Internet should ideally be supervised by an adult at all times, and particularly when using iPads on the C2k Wireless network.
- All pupils are aware of the rules for the safe and effective use of the Computers/iPads. These are displayed in the ICT Room and P3-P7 classrooms and are routinely discussed and reinforced with pupils.
- All pupils using the Internet have permission from their parent/guardian. This may be given as written or digital permission.
- Equipment, websites, Apps and materials recommended for use of pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate, especially if these have been downloaded from a non-C2k filtered network.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinators.
- In the interests of system security staff passwords should only be shared with the network manager.
- Teachers are aware that the C2k system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users. Security reports can be requested by the Principal if necessary.
- Teachers should be aware of copyright and intellectual property rights, and should be careful not to download or use any materials which are in breach of these.
- Photographs and videos of pupils should, where possible, be taken with school equipment and images should be stored on the school network, school MacBook Pros or on school provided, encrypted memory sticks accessible only by staff.
- Staff members secure their school iPads with a passcode, and these iPads should not be for pupil use.
- All school documents and staff/pupil information should be stored on encrypted memory pens if being used outside of school.
- School systems may not be used for unauthorised commercial transactions.
- Staff will read and sign the Staff User Agreement for Internet Access (*Appendix 5*).

3. Online Safety Awareness

In Ballykeel PS & NU we believe that, alongside having written policies on Online Safety and Acceptable Use of the Internet & Digital Technologies (which includes a Code of Practice), it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. Children also need to be educated about how to recognise and avoid the risks, in an age-appropriate manner. They need to know how to cope if they come across inappropriate material or situations online and should be encouraged to seek help and advice when they need it without fear of censure or criminalisation. We see this as an essential element of the school curriculum, and this education is as important for staff and parents as it is for pupils.

3.1 Online Safety Awareness for pupils

Rules for Online Safety and Using Computers/iPads are discussed with pupils and are prominently displayed in the ICT Room and classrooms. 'SMART' tips are also discussed with the children and displayed. Teachers make use of the lessons and resources provided by Safer Schools NI portal/app, and resources from the UK Safer Internet Day website, to deliver Online Safety lessons. Visitors are also brought in to run workshops with KS2 children where possible.

Children are made aware of the Online Safety Team in school every year. Posters of the relevant staff are displayed in each classroom and pupils are encouraged to speak to the Online Safety team for support or to report an incident.

3.2 Online Safety Awareness for Staff

The ICT Co-ordinators and Designated Teacher for Child Protection are kept informed and updated on issues relating to Online Safety and attend regular courses. This training is then disseminated to all teaching staff, classroom assistants and supervisory assistants on a regular basis. Online Safety training workshops are held for staff as appropriate.

3.3 Online Safety Awareness for parents/guardians

Ballykeel PS & NU aim to share information, advice and guidance on the appropriate and safe use of digital technology with parents/guardians on a regular basis. The Online Safety Policy and Code of Practice for pupils (Rules for Using the Computers/iPads in School) are available on the school website (www.ballykeelps.org.uk). An Online Safety Advice leaflet is also included as part of our P1 Induction Pack and is sent out again in P4. It will also be given to parents of new pupils joining the school in other year groups. 'Online Safety Shout-outs' are sent out to Parents via the school bulletin/website. Online Safety Information sessions are also provided for parents/carers, delivered by school/outside agencies e.g. PSNI, NSPCC, Barnardos. Parents have also been advised of the Safer Schools NI App and website.

4. Health and Safety

Ballykeel PS & NU has attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, in classrooms, Resource Areas and the ICT Room. Pupils are supervised at all times when Interactive Panels are being used.

5. Digital and Video Images of Pupils

Parental permission is sought annually to cover the use of photographs and names of pupils on the school website, Seesaw, in the local press and for displays within school, and written permission must be obtained from a parent/carer. The child should be tagged by his/her first name only.

5.1 School Website

Our school website provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions;
- The website does not include photos with surnames, home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.
- A child will not be photographed for the website without written consent from a parent/carer.
- Certain areas of the school website are only accessible to parents via a password.

5.2 Seesaw

The school uses the website/app Seesaw to communicate instantaneously with parents. This includes sending of whole class, group and individual information in the form of inbox messages, and the use of the Journal section to send individual, group and whole class posts containing photographs, samples of work and messages about a child's learning.

Annually, parents/carers will be asked to give permission for photographs, videos and voice recordings of their child, and samples of their work, to be taken and used within the Seesaw App (in individual, group and whole class postings).

5.3 Storage of images

Digital and video images of pupils are taken with school equipment, preferably the designated 'teacher iPads'. Images are stored on the school network, school

MacBook Pros or school provided encrypted memory sticks, accessible only by staff. Photographs of pupils should be removed from computers, iPads and memory sticks when they leave the school.

6. Social Software

Chat Rooms, blogs and other social networking sites are blocked by the C2k filters, so pupils do not have access to them in the school environment. However, we regard the education of pupils in the safe and responsible use of social software as vitally important and this is addressed through Online Safety lessons.

Safe social interaction is encouraged through use of Newsdesk, a digital resource allowing pupils to have their comments published (filtered and edited by C2k). This gives children positive experiences when exchanging ideas and sharing opinions online. Older pupils can also communicate with each other using Google Classroom, which has been set up and is monitored by the class teacher.

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's Positive Behaviour Policy, Social Media Policy and Child Protection procedures; and recorded as per the Anti-Bullying Policy.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

7. Mobile Technologies

The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material. Staff should not store pupils' personal data and photographs on personal memory sticks which are taken off school premises. Pupils are not allowed to use personal mobile devices/phones in school or on trips. Staff should not use personal mobile phones during designated teaching sessions.

8. Managing Video-conferencing

Video-conferencing will be via the C2k network to ensure quality of service and security, and will be appropriately supervised.

9. Policy Communication and Parental Agreement

Having read the school's Acceptable Use of the Internet and Digital Technologies Policy and Code of Practice for pupils (Rules for Using the Computers/iPads in School), parents in P1 are asked to complete and return the Rules for Using Computers/iPads in School Permission Form on behalf of their child. Parents in P4 are asked to discuss the Rules for Using the Computers/iPads in School with their child, and both the parent and child should sign and return the Permission Form. Forms will be issued accordingly to new pupils as they join the school. If necessary, permission may also be given by parents/guardians via Seesaw/email.

10. Monitoring and Review

This policy is implemented on a day-to-day basis by all school staff, and is monitored by the ICT Co-ordinators. Due to the ever-changing nature of the Internet and digital technologies, this policy and its effectiveness will be reviewed annually.

Policy reviewed by Mrs B Esler and Miss L Kane, ICT Co-ordinators, September 2023.

Online Safety Policy

This policy is based upon the following DENI Circulars: 2016/27 on Online Safety, 2013/25 on e-Safety Guidance, 2011/2 on Internet Safety and 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and operates in conjunction with Ballykeel Primary School's Acceptable Use of the Internet and Digital Technologies Policy

1. Introduction

"Schools play a crucial role in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and educating children and young people about how to act appropriately and stay safe."

(DENI Curricular 2016/27)

In Ballykeel Primary School and Nursery Unit we are aware of our responsibility to educate pupils and provide them, and parents, with information relating to Online Safety. Our aim is to teach children about appropriate online behaviours, and to think carefully about various situations to help them remain safe and legal when using the Internet and related digital technologies both in school and at home.

2. What is Online Safety?

- Online safety means acting and staying safe when engaging in the online world. It is wider than simply internet technology and includes electronic communication via text messages, social media environments, online platforms and apps; and using games consoles through any digital device.
- It is about using digital devices in a smart but safe way. It means educating children and young people to act responsibly and keep themselves safe in the digital world.
- It highlights the responsibility of the school, all Staff, Governors and parents to mitigate risk through reasonable planning and actions. In all cases, in schools and elsewhere, Online Safety is a paramount concern.

Within Ballykeel PS, Online Safety:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and

- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

3. Education of Pupils in Online Safety

The Internet is an integral part of pupils' lives, both inside and outside school. There are ways for pupils to experience the benefits of communicating online with their peers in relative safety. However, young peoples' extensive use of technology leaves no doubt over the importance of online safety. The Internet is an open communications channel and as such children can come into contact with people from all sectors of society, and a wide variety of communications and materials which may not always be suitable. Risks include:

(i) Potential Contact

Children may come into contact with someone online who may wish to harm them. Inappropriate contact may be initiated via social networking sites, chat rooms, email or online games.

At Ballykeel PS & NU we recognise it is important to educate our children to know:

- People are not always who they say they are online;
- 'Stranger Danger' also applies to people they meet on the Internet;
- They should never give out personal information online such as full names, ages, addresses, school name, siblings etc.;
- They should never meet alone anyone they have met through an Internet source;
- Once information is published online it can be disseminated with ease and cannot be easily destroyed, with particular reference to photographs.

(ii) Inappropriate Content

Unsuitable, inappropriate and harmful materials appear on the Internet in a variety of formats. Some material is published for an adult audience and is therefore unsuitable for children e.g. materials with a sexual content. Other materials may express extreme views that cannot be published elsewhere e.g. regarding racism, crime, weapons. Materials can also be harmfully inaccurate and misleading e.g. promotion of harmful activities such as anorexia or bulimia, drugs etc.

In Ballykeel PS & NU we aim to teach our children:

- That not all information available on the Internet is true or accurate;
- That they should question the source of the information they are accessing;
- To know how to respond to unsuitable materials or requests, and to immediately tell a teacher or appropriate adult.

(iii) Excessive Commercialism

The Internet is a powerful vehicle for advertising. Many websites which our children will visit will feature advertising which is very persuasive, or the advertising may be inappropriate. Websites may also expose them to marketing schemes or hidden costs/fraud.

In Ballykeel PS & NU we aim to teach our children:

- Not to fill out forms requiring a lot of personal details without permission from an appropriate adult;
- Not to order products online or Apps without first seeking permission from a parent/carer.

As children have access to the Internet in a variety of places other than school it is important that we educate them in how to behave appropriately online, and to understand the importance of discussing problems and issues that might arise. It is also important that all staff, parents and carers must be vigilant when children are using the Internet in school, particularly when on the C2k wireless network.

(iv) Cyber-bullying

Staff in Ballykeel PS & NU are aware that pupils may face conduct risks when online, either as a perpetrator or the target of bullying behaviour in peer-to-peer exchanges, and/or are at risk of entrapment and/or blackmail. Cyber-bullying via any electronic methods of communication (including online games and mobile phones) may occur both in and out of school. This form of bullying is addressed within our school's Anti-Bullying Policy and through our pastoral services, as well as the Online Safety Policy and Social Media Policy if applicable.

Social media is rarely used for learning and teaching within Ballykeel PS & NU, but we recognise it is important that our children are educated about the risks and issues related to social media. Each of the social media technologies can offer much to schools and pupils, but each brings its own unique issues and concerns. Therefore, staff considering using social media should first discuss this with the ICT Co-ordinators. The school's Social Media Policy should also be taken into consideration if exploring social media with pupils.

Cyber-bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments about another user, or on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi- player gaming sites.

- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abuse of Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following are some of the Orders which may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997 http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988 http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003 http://www.legislation.gov.uk/ukpga/2003/21

In Ballykeel PS & NU pupils and parents are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases. Incidents of cyber-bullying are recorded and monitored by the Online Safety Team in an 'Online Safety Risk Register', and will also be recorded and monitored in accordance with the school's Anti-Bullying Policy by the Principal. Pupils should be made aware of the importance of not immediately deleting 'evidence', but instead passing it on to a trusted adult when reporting the incident; and that they should not pass messages on to others.

To help children recognise and avoid these four identified areas of risk and how to cope if they come across inappropriate material or situations online, and to promote the importance of a positive digital footprint, Online Safety Rules (*Appendix 1A & 1B*) and Rules for Using Computers/iPads (*Appendix 3)* will be displayed in all classrooms and the ICT Room, along with 'SMART' tips (*Appendix 2)* for staying safe online. These will be discussed with the pupils at the start of each year and reminders issued each term. Throughout the year P1-P7 teachers will teach specific lessons based on Online Safety, making use of resources provided by Safer Schools NI portal/app. As a whole school we participate in Safer Internet Day annually, using the theme and resources from the UK Safer Internet Day website. *Appendix 6* is a list of suggested websites providing materials for delivering Online Safety messages across all year groups. The children will also be made aware of who the Online Safety Team is in school.

Pupils will also be informed that their C2k network and Internet use will be monitored through Securus.

4. Online Safety Information for Parents/Carers

It is important to note that schools cannot cover every Online Safety scenario and that parents have the primary responsibility for the protection and safeguarding of their children. We recognise the reality is that many parents are intimidated by the complexity of modern technologies, and may feel inadequate in the face of the ready familiarity with which their children use them. In Ballykeel PS & NU, we aim assist parents/carers by:

- Asking them to read through the Rules for Using Computers/iPads in School along with their child and sign the Permission Form in P1 (*Appendix 4A*) and again in P4 (*Appendix 4B*). Parents of new pupils in other year groups will be asked to do likewise when they join the school.
- Asking them to make a decision as to whether they consent to images of their child being taken/used on the school website.
- Communicating relevant Online Safety information through the school website, Seesaw, Bulletins, letters and a Parental Advice booklet issued to parents when pupil enter P1, P4 or when they join the school for the first time.
- Inviting outside agencies into school to provide training for parents/carers in the area of Online Safety where possible.
- Informing parents/carers of dangerous/inappropriate websites/Apps as deemed necessary through 'Online Safety Shout-outs' sent via the Schools NI App or via Seesaw.
- Sharing Online Safety information on a dedicated page on the school website, including links to useful websites, e.g. Safer Schools website and UK Safer Internet Centre.
- Asking them to model appropriate behaviour when online.

Parents should remember that it is important to promote Online Safety in the home and to monitor Internet use. The following advice may be useful:

- Keep the computer/tablet in a communal area of the home.
- Be aware that children have access to the Internet via gaming consoles and portable technologies such as smart phones and watches.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what the children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social-networking sites/games which are unsuitable for them to be accessing.
- Discuss how the children should respond to unsuitable materials or requests – stress the importance of immediately telling a trusted adult at home or in school rather than trying to delete potential evidence for fear of getting into trouble.

- Remind the children never to give out personal information online.
- Remind the children that people online may not be who they say they are.
- Be vigilant. Ensure that the children do not arrange to meet someone they meet online.
- Be aware that the children may be using the Internet in places other than in their own home or at school, and that this Internet use may not be filtered or supervised.

5. E-mail Security

C2k provide all staff and pupils with email accounts, and it is recommended that only the C2k email system be used for school emails. Email accounts are only authorised for use by our P6 and P7 classes (if necessary), and are only used with the permission of the teacher. Pupils must not send out personal information about themselves or others in an email, unless given permission by a teacher.

The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content. However, should a pupil receive an email they feel is offensive, they should inform a teacher immediately.

Staff are strongly advised to use their C2k email account for school business only; and to communicate with parents/guardians via Seesaw rather than email.

6. Internet Security

In Ballykeel PS & NU, Staff and pupils can only access the Internet via the C2k Education Network. To do so they are required to authenticate log-in using their C2k username and password. This authentication provides Internet filtering via the C2k Education Network solution for the protection of staff and pupils alike. The C2k Wireless Network is used to provide Wi-Fi for School-Based Digital Technologies such as iPads and a MacBook. Arbitration requests may be submitted to C2k to allow the school to have access to specific, previously blocked websites.

Access to the Internet via the C2k Education Network is fully auditable and reports are available for the school Principal.

7. Securus Education Software

To ensure that we are effectively monitoring and safeguarding the children's use of information systems and electronic communications, Securus Education software has been deployed on all C2k managed devices. This software alerts staff when evidence presents of bullying, inappropriate language or searches for inappropriate

websites. A screen 'capture' is taken of each incident; recording the user details, time and date of the incident. These captures are monitored by the Online Safety Team who then can respond to any incidents which have occurred.

8. Professional Development for Staff

Teaching and non-teaching staff are the first line of defence in Online Safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Online Safety training is therefore an essential element of staff induction and Continual Professional Development.

This can be achieved by:

- Ensuring all staff receive regular information and training on Online Safety issues through the ICT Co-ordinators.
- Making all staff aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety, and to know what to do in the event of misuse of technology by any member of the school community.
- Ensuring new staff members receive information on the school's Acceptable Use Policy and Online Safety Policy as part of their induction.
- Staff incorporating Online Safety activities and awareness within their lessons, using the resources available on Safer Schools NI, and the Safer Internet Day website.
- Advising staff of C2k resources on Online Safety.
- Incorporating Online Safety training as part of CPD when appropriate.
- Requesting additional support and advice from C2k, Social services, PSNI or other outside agencies when required.

9. Management of Personal Data

Personal data belonging to pupils, parents and staff is collected and managed responsibly in line with relevant legislation (Data Protection Act 2018 and Freedom of Information Act 2000), and staff are trained annually in GDPR guidelines and good practice. An Information Asset Register outlines who has access to different pupil and staff data held electronically in school.

If technology is being used to communicate between school and pupils, their families/carers and external agencies, this should be clear and professional.

C2k provides the infrastructure and services to support the enhanced use of ICT in schools in Northern Ireland. C2k's single Education Network for NI provides all grant-aided schools with an integrated suite of technologies and opportunities to extend learning across local and wider communities. These include:

MySchool – *A personalised learning and working environment for pupils and teachers*
C2k Newsdesk – *A news and curriculum service with content created specifically for children*
Textlocal – *A texting (SMS) solution within MySchool*
C2K Media Library – a range of videos and resources for Online Safety messages
Office 365 – *Office web applications*
G-Suite – *Google web applications*
Partnership exchange – *An application to support the sharing of student data within Area Learning Communities*

In order to provide these services effectively, a limited amount of school data is shared with suppliers in order to integrate their products within the MySchool portal. All sharing is conducted under contract with suppliers, with provisions in place to ensure information security.

10. Risk Assessments

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity, they will need to learn to recognise and avoid these risks – to become "Internet-wise" and ultimately good "digital citizens". In Ballykeel PS risk assessments are carried out on the technologies used within school to ensure we are fully aware of and can mitigate against the potential risks involved with their use. Our aim is to teach our pupils how to cope if they come across inappropriate material or situations online. Risk Assessments are referred to in the Acceptable Use of the Internet and Digital Technologies Policy (Code of Practice for Staff).

11. Reporting and Handling Online Safety Concerns

Concerns regarding misuse of the Internet or Digital Technologies will be dealt with by the Online Safety Team. Incidents of deliberate access to inappropriate materials by any user or potential breaches of online safety/data security will be recorded by the Online Safety Team in an 'Online Safety Risk Register'. Concerns regarding inappropriate online material found on the C2k network will be reported to C2k/Capita immediately. Evidence of concerns should be retained so it can be recorded and/or passed to relevant agencies/authorities, unless doing so would be immediately detrimental to pupils (e.g. if something inappropriate appeared on an IWB/panel, or was visible to others in the ICT Room). Concerns regarding a breach of data should be reported immediately to the Principal.

Concerns of a Child Protection nature will be reported to a Designated or Deputy Designated Teacher and dealt with in accordance with our Child Protection Policy.

Concerns about Staff misuse of the Internet or Digital Technologies will be referred to the Principal.

12. Communication of the Online Safety Policy

This Online Safety Policy has been developed by the ICT Co-ordinators and agreed by staff and the Board of Governors. It will be available for viewing on the school website www.ballykeelps.org.uk, and copies will also be available from outside the Office. The Online Safety Policy will be reviewed annually, and parents will be informed when this happens.

Policy reviewed by Mrs B Esler and Miss L Kane, ICT Co-ordinators, September 2023.

P1-3 Online Safety Rules

'Think then Click'

These rules help us to stay safe on the Internet

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly messages to people that we know.

P4-7 Online Safety Rules

'Think then Click'

These rules help us to stay safe on the Internet

We ask permission before using the Internet.

We only use websites that an adult has chosen, unless we are asked to do independent research.

We tell an adult if we see anything we are uncomfortable with.

We immediately close any webpage we not sure about.

We only e-mail or message people an adult has approved.

We make sure emails and messages are polite and friendly.

We never give out personal information or passwords.

We never arrange to meet anyone we don't know.

We do not open e-mails sent by anyone we don't know.

We do not use Internet chat rooms or social networking sites in school.

Appendix 2

Follow These SMART Tips When Online

S **Secret -** Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

M **Meeting** someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

A **Accepting** e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

R **Remember** someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!

T **Tell** your parent or carer if someone or something makes you feel uncomfortable or worried.

Appendix 3

Ballykeel Primary School & Nursery Unit
Rules for using Computer/iPads

- On the C2k network, I will only use my own login username and password.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will use the Internet for research and school purposes only.
- I will ask permission before entering any website, unless my teacher has already approved that site or has asked me to do independent research.
- I will only send e-mail which my teacher has approved, and I will make sure that the messages I send are polite and responsible.
- I will not use inappropriate language, nor will I retrieve, send, copy or display offensive messages or pictures.
- When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
- I will not open email or attachments from someone I do not know.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I will immediately report any pop-up boxes which I do not understand.
- I understand that I am not allowed to enter Internet Chat Rooms or Social Networking Websites while using school computers or iPads.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I will not bring in memory sticks or digital/electronic devices unless I have been given permission to do so by my teacher.
- I will not deliberately waste resources, such as printer ink and paper.
- I will treat all equipment with respect and will not deliberately damage it.
- I understand that breaking any of these rules may result in me not being allowed to use the Internet, computers or iPads.

Appendix 4A (P1-3)

Ballykeel Primary School & Nursery Unit
Rules for using Computer/iPads
PERMISSION FORM

P1-P3

Children should understand that they are responsible for using the Internet and Digital Technologies responsibly. Please read the rules carefully and talk to your child about using Computers/iPads safely in school. This form should then be signed by a parent/carer and returned to the class teacher.

Pupil's Name	
Class Teacher	
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions. I also understand that despite filtering provided by C2k, some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.	
Name of Parent/ Guardian (print)	
Signature of Parent/ Guardian	
Date	

Appendix 4B (P4-7)

Ballykeel Primary School & Nursery Unit
Rules for using Computer/iPads
PERMISSION FORM

P4-P7

Children should understand that they are responsible for using the Internet and Digital Technologies responsibly. Please read and discuss these rules with your child, and ensure you both sign them in the spaces provided. Forms should then be returned to the class teacher.

Pupil's Name	
Class Teacher	
As a school user of the Internet, I agree to follow the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by my school. I will use computers and all other digital equipment sensibly.	
Pupil's Signature	
Date	

Pupil's Name	
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email and Google Classroom (P6/P7 only). I understand that pupils will be held accountable for their own actions. I also understand that despite filtering provided by C2k, some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.	
Name of Parent/ Guardian (print)	
Signature of Parent/ Guardian	
Date	

Appendix 5

Ballykeel Primary School & Nursery Unit
Staff User Agreement for Internet Access

The C2k Computer Network and school iPads may be accessed by Staff their professional activities including teaching, research, administration and management. The school's Online Safety, Acceptable Use of the Internet and Digital Technologies, and Social Media Policies have been drawn up to protect all parties – the students, the staff and the school.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the ICT Co-ordinators.

- All Internet activity should be appropriate to staff professional activity or the pupils' education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Documents containing personal data related to staff/pupils should be saved on the school ICT system, or on school provided encrypted memory sticks.
- Teacher iPads should have a secure password and not be used by pupils.
- Use of the Internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited – requests for these reports may be made to C2k by the Principal.
- Personal mobile digital devices brought into school are subject to the same Code of Practice requirements as School-Based technology.

Staff Name: _____

Staff Signature: _____

ICT Co-ordinator Signature: _____

Date: _____

Appendix 6

Ballykeel Primary School & Nursery Unit

Suggested resources for teaching Online Safety

C2k can offer advice on internet safety and has produced resources including 'Better safe than sorry' and 'Internet Safety Room'.

A number of other organisations can offer support and resources including:

- Think u know: Child Exploitation and Online Protection Command (CEOP) 'thinkuknow' website contains advice and resources for teachers exploring the risks which children and young people are exposed to. CEOP has produced targeted advice and guidance for Key Stages, Resources and guidance for parents/carers, and teachers is also available:
- Get Safe Online provides useful advice and information on how to stay safe online. Safeguardingni.org will also provide information for parents and carers on online safety.
- UK Safer Internet Centre offers online safety tips, advice and resources to help professionals, children and young people to stay safe on the internet.
- Safer Schools NI provides safeguarding and child protection support for school staff, parents/carers and pupils.
- NI Online Safety Hub provides helpful advice and resources to keep young people safer online.
- NSPCC Share Aware
- Netware app guidance
- ChildNet
- Childnet "Trust Me" Critical Thinking Resources
- EA Digital Safeguarding Resources
- Be Internet Legends

(These are available to staff as direct links in the Online Safety Folder found in the Public Folder).