Contents

1. Roles and responsibility 6

E- Safety Team 6

E-Safety Coordinator 7

Board of Governors 7

Principal 8

Teaching and Support Staff 8

Designated Teacher for Child Protection 8

Pupils 9

Parents / Carers 9

2. Communicating school policy 10

3. Making use of ICT and the internet in school 11

E-Safety and Pupils 12

E-Safety and Staff 12

E-Safety and Parents / Carers 13

4. Managing information systems 14

Internet Security– C2K 14

Password Security 14

Acceptable internet use 15

5. Emails 16

6. School website 16

6.2 Social networking, social media and personal publishing 17

7. Cyberbullying 18

8. Mobile phones and personal devices 20

8.2. Managing emerging technologies 21

Appendices 21

Pupil Acceptable Use Agreement Template – for older pupils 22

Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1) 24

Staff (and Volunteer) Acceptable Use Policy Agreement Template 26

Parent / Guardian Acceptable Use Agreement Template 29

Responding to incidents of misuse – flow chart 31

Record of reviewing devices/internet sites (responding to incidents of misuse) 33

E-safety Incident Report Form 34

**E-SAFETY POLICY**

Omagh County Primary School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a ‘duty of care’ for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

To deal with any incidents of technology misuse by pupils which arise, the school’s Positive Behaviour Policy will be followed. Pupils must be made aware the repeated misuse of the Internet may lead to their access to it being denied. If a member of staff is involved, then the disciplinary procedures for employees of the school will be followed.

Where the incident involves child abuse, the Designated Teacher for Child Protection in the school must be notified and the school will follow procedures as set out in the school’s Safeguarding and Child Protection Policy.

Issues of Internet misuse and access to any inappropriate material by any user should be reported immediately to the school’s e-Safety Co-ordinator and recorded in the school’s e-Safety log, giving details of the site and the time.

A record of very serious incidents will be kept in the locked Child Protection cabinet within school.

Harassment of another person using technology or breaching their right to privacy (e.g. reading their mail, accessing their files, using their computer account or electronic mail address), poses a threat to their physical and emotional safety, and may have legal consequences.

For these purposes, it is also essential that evidence of misuse is secured. If the school identifies a suspect device (containing for instance indecent images or offences concerning child protection), it will not be used or viewed, and advice will be sought from the P.S.N.I.

After a minor or major incident, a comprehensive debriefing will occur to review school policy and procedures.

Logs of misuse are made available to the:

* Senior Leadership Team;
* Principal;
* Governors or governors’ sub-committee;
* e-Safety Team.

If police involvement is necessary, the Principal and Board of Governors will seek advice from School’s Branch and the legal department at the Education Authority (Western Region).

ILLEGAL or INAPPROPRIATE ACTIVITIES

The school believes that the activities listed below are inappropriate (and on occasions illegal) in a school context and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

* child sexual abuse images (illegal - The Protection of Children Act 1978); grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003);
* possession of pornographic images (Illegal – Public Order Act 1986);
* promotion of any kind of discrimination (illegal – Criminal Justice and Immigration Act 2008 criminally racist material in UK – to stir up religious hatred or hatred on the grounds of sexual orientation);
* promotion of racial or religious hatred;
* threatening behaviour, including promotion of physical violence or mental harm;
* any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally, the following activities are also considered unacceptable on school ICT equipment provided by the school:

* using school systems to run a private business;
* use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by C2K;
* uploading, downloading or transmitting commercial software or any copyrighted
* materials belonging to third parties, without the necessary licensing permissions;
* revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords);
* creating or propagating computer viruses or other harmful files;
* on-line gambling and non-educational gaming;
* use of personal social networking sites/profiles for non-educational purposes.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. 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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

## **Roles and responsibility**

## E- Safety Team

The E-Safety Team provides a consultative group that has representation from the school community, with responsibility for issues regarding online safety and the monitoring of the E-Safety Policy including the impact of initiatives. Members of the E- Safety Team will assist the E-Safety Coordinator with:

* the production / review / monitoring of the school E- Safety Policy and other documents.
* monitoring improvement actions identified through use of the 360-degree safe self-review tool

The school’s E-Safety Team consists of:

* Miss Funston - Principal
* Miss Beattie - ICT Coordinator & E-Safety Coordinator
* Mr Morgan - C2K Manager
* Mrs A Dempsey – Vice Principal/ Designated Teacher for Child Protection
* Mrs E Alcorn - Deputy Designated Teacher for Child Protection

Children

* Mr Morgan’s Yr. 7 class

## E-Safety Coordinator

* leads the E-Safety Team
* takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
* ensures that all staff are aware of the procedures (see flow chart in appendix) that need to be followed in the event of an online safety incident taking place
* provides training and advice for staff
* liaises with the Education Authority
* receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
* reports regularly to the Senior Leadership Team
* receives appropriate training and support to fulfil her role effectively
* passing on requests for blocking/unblocking internet sites to the C2K helpdesk
* liaises with the Safeguarding and Child Protection Team

## Board of Governors

* The governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. They should receive regular information about e-safety incidents and monitoring reports.

## Principal

* The Principal has a duty of care 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 E-Safety Coordinator.
* The Principal and another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents in appendix).
* The Principal is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

## 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 E-Safety Policy and practices
* they have read, understood, and signed the Staff Acceptable Use Policy
* they report any suspected misuse or problem to the Principal; E-Safety Coordinator or member of the Safeguarding Team for investigation
* all digital communications with parents / carers should be on a professional level and only carried out using official school systems
* online safety issues are embedded in all aspects of the curriculum and other activities
* pupils understand and follow the E-Safety Policy and acceptable use policies
* they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices, see Acceptable Use for Mobile Phones and Related Technologies Policy.

## Designated Teacher for Child Protection

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

(It should be noted that these are safeguarding issues, not technical issues; the technology provides additional means for safeguarding issues to develop and therefore a member of the Safeguarding and Child Protection Team should form part of the E-Safety Team.)

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

## Pupils

* are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
* 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-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. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at school events
* access to parents’ sections of the website

## **2.** **Communicating school policy**

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed in the computer room. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PDMU lessons where personal safety and responsibility are being discussed.

## **3. Making use of ICT and the internet in school**

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

**For pupils:**

* Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
* Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
* Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
* An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
* Access to learning whenever and wherever convenient.
* Freedom to be creative.
* Freedom to explore the world and its cultures from within a classroom.
* Social inclusion, in class and online.
* Access to case studies, videos and interactive media to enhance understanding.
* Individualised access to learning.

**For staff:**

* Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
* Immediate professional and personal support through networks and associations.
* Improved access to technical support.
* Ability to provide immediate feedback to students and parents.
* Class management, attendance records, schedule, and assignment tracking.

E-Safety in Omagh County Primary School depends on effective practice at a number of levels:

* responsible ICT use by all staff and students; encouraged by education and made explicit through published policies;
* sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use;
* safe and secure internet provision delivered and managed by C2K.

## E-Safety and 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 online safety is therefore an essential part of the school’s online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

* Key online safety messages should be provided as part of ICT and PDMU lessons and should be regularly revisited.
* Pupils should be taught in all lessons to be critically aware of the content they access on-line.
* Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
* Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
* 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-flow chart.
* Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
* Where pupils are accessing the internet through iPads, which is unsecured and therefore not filtered by C2K, they should use the search engine Swiggle which filters content.

## E-Safety and Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

* The E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from C2K /EA) and by reviewing guidance documents released by relevant organisations.
* This E-Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
* Staff will be asked to read and sign the Acceptable Use of the Internet Agreement for Staff (see appendix) which focuses on e-safety responsibilities in accordance with the Staff Code of Conduct.
* Staff using their own digital cameras or mobile telephones in exceptional circumstances to take photographs or video footage should transfer the images/footage as soon as possible to the school’s C2K system and then delete them from the camera, mobile phone or similar device.
* Staff have access to YouTube (for educational purposes only) when logged into C2K system. Therefore, staff must ensure that no pupil is given access to a computer that they are logged on to unless being supervised.
* Staff should always ensure that any Internet searches involving sites that have been granted enhanced access to should not be carried out when children can view them, i.e. on the computer’s screen or on an interactive whiteboard. YouTube should only be used after the content has been viewed and checked, ensuring that children are not exposed to inappropriate content.

## E-Safety and Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

* Curriculum activities
* Provide access to this E-Safety policy on the website.
* Letters, newsletters, web site
* High profile campaigns e.g. Safer Internet Day
* Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

## **4. Managing information systems**

## Internet Security– C2K

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution protecting users and systems from abuse. Pupils must not use any personal electronic devices within school to access the internet or any messaging services without prior permission from a member of staff.

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

Connection of non C2K devices to the Internet e.g. iPads and other personal devices through the controlled C2K guest wireless network is not subject to the same level of filtering as the main school system. When pupils access the internet through iPads, they should use the search engine Swiggle which filters content. This has been bookmarked on each iPad and is the responsibility of the staff to direct pupils to use this search engine.

The school takes the protection of school data and personal protection of our school community very seriously. In addition to the security offered by the C2K network some safeguards that the school takes to secure our computer systems are:

* the use of user logins and passwords to access the school network will be enforced
* portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

## Password Security

* Staff users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils, and should be changed if it appears pupils have worked out an adult’s password.
* All pupils are provided with an individual login username and password.
* Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
* Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

## Acceptable internet use

* The C2K computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school’s e-Safety policy has been drawn up to protect all parties – the students, the staff and the school.
* The school reserves the right to examine and delete any files that may be held on its computer system or to monitor any Internet sites visited.
* Staff should read and sign a copy of the school’s Acceptable Internet Use Agreement for Staff and return it to the Principal (refer to appendix).
* The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety.
* Educating pupils on the dangers of technologies that may be encountered outside of school will be discussed with pupils in an age appropriate way on a regular basis by teachers and other agencies (as appropriate – e.g. PSNI as part of the CASE project).
* Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of how to seek advice or help if they experience problems when online, e.g. from a parent/carers, teacher/trusted member of staff.
* The school internet access is filtered through the C2K managed service;
* Use of the internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
* Pupils will be taught to use the internet as an aid to learning.
* The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
* Children will be taught to be ‘Internet Wise’ and therefore good online citizens. and are encouraged to discuss how to cope if they come across inappropriate content.

## **5. Emails**

The school uses email internally for staff, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

* initiating contact and projects with other schools nationally and internationally
* providing requests for support where it is needed.

Staff should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

**Staff should be aware of the following when using email in school:**

* Staff should only use official school-provided email accounts to communicate with parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
* Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
* Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
* The forwarding of chain messages is not permitted in school.

## **6. School website**

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. 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;
* Only photographs of children with parental/carer consent will appear on the school’s website.
* Names will be included with photographs on the website only if parent/carer permission has been given;
* The website does not include home addresses, telephone numbers, personal e-mail or any other personal information about pupils or staff.
* The point of contact to the school i.e. school telephone number, school address and email address.

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

Social software is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and blogs (personal web journals).

Social environments enable any community to share resources and ideas amongst users. There are many excellent public examples of social software being used to support formal and informal educational practice amongst young people and amongst educators. They are also popular ways of enabling users to publish and share information, including photographs, video from webcams, video files and blogs about themselves and their interests.

C2k filters out services which are misused and block attempts to circumvent the filters. Pupils will not be allowed to use any social software which has not been approved by teaching staff and the C2K filtering service.

Staff and pupils are advised that it is not acceptable or school policy for them to be friends on social network sites (e.g. Facebook). Pupils in this school are told they should not request to be friends with a member of staff on a social network site. Equally, staff are also told that they must not request to be friends or accept requests to be friends with pupils or past pupils of the school on any such site. This is good practice in line with child protection/safeguarding children policy.

* The school C2K systems deny access to social networking sites.
* Pupils and their parents/carers are advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
* Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
* Cyber-bullying is addressed within this policy and staff are made aware that pupils may be subject to cyber-bullying via electronic methods of communication both in and out of school. (More information provided below).
* Our pupils are asked to report any incidents of cyber-bullying to the school.

Social networking through the use of Internet-based and other electronic social media tools is integrated into everyday life. Use of Facebook, Twitter, blogging, wikis and other online social media vehicles are now commonplace with the result that the lines between work and personal life can become blurred. To protect staff, pupils and the reputation of the school the following guidelines should be followed:

* Staff should not use school systems to engage in personal social media activities, i.e. Facebook, Twitter, blogging, wikis etc. This inappropriate use of social media sites may be treated as a disciplinary matter;
* If staff use social media sites for personal use, they are reminded that they have a responsibility to ensure they are posting comments or images that are not detrimental to their position as a staff member of Omagh County Primary School, the privacy or rights of pupils or the reputation of the school. Images may include photographs from staff parties that could be misinterpreted and present the staff or the school, in a negative light. A common sense approach to the use of social media websites is recommended.

## **7. Cyberbullying**

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the **Positive Behaviour Policy and Anti-Bullying Policy.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

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 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;
* Abusing 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 may cover different elements of cyber-bullying behaviour:

It is important that pupils 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.

* A record is kept of all incidents of cyber-bullying and reported to the e-Safety team. This allows the schools e-Safety team to monitor the effectiveness of the school’s preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

If an allegation of bullying does come up, the school will:

* take it seriously
* act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
* record and report the incident
* provide support and reassurance to the victim
* make it clear to the ‘bully’ that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the ‘bully’ will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

## **8. Mobile phones and personal devices**

It is important to be aware of the safety issues regarding mobile phones and other devices which now increasingly have Internet access. For this reason, Omagh County Primary School has a specific policy on the **Acceptable Use of Mobile Phones and Related Technologies** which should be referred to.

## **8.2. Managing emerging technologies**

Technology is progressing rapidly, and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

**POLICY REVIEW**

This e-Safety policy and its implementation will be reviewed annually or updated when new technologies are introduced and after a risk assessment has been completed.

**Signed by**

**Chair of governors**

**Date: ...............................**

**Principal**

**Date: ..................................**

# Appendices

Appendices 21

Pupil Acceptable Use Agreement Template – for older pupils 22

Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1) 24

Staff (and Volunteer) Acceptable Use Policy Agreement Template 26

Parent / Guardian Acceptable Use Agreement Template 29

Responding to incidents of misuse – flow chart 31

Record of reviewing devices/internet sites (responding to incidents of misuse) 33

# Pupil Acceptable Use Agreement Template – for older pupils

**School policy**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Young people should have an entitlement to safe access to these digital technologies.

Children should be taught from P1 – P7 that they are responsible for their use on the Internet in school and that they should use it in a safe, responsible, and appropriate manner. The following guidelines are shared and discussed with the pupils in an age appropriate way.

**Staff should continually teach and stress the importance of safe use of the internet.**

**WHEN USING THE C2K SYSTEM PUPILS SHOULD:**

* only use their own login username and password;
* use the Internet for school/educational purposes only;
* tell a teacher immediately if he/she sees anything that they consider inappropriate or receive messages they do not like;
* only send e-mail or any other form of electronic communication in school when directed by the teacher;
* make sure any internet based communication is polite and responsible;
* understand that if they consistently choose not to comply with these expectations they will be warned and subsequently may be denied access to Internet resources;
* understand that the school may check their computer files/e-mails and may monitor the Internet sites that they visit when on school systems.

**WHEN USING THE C2K SYSTEM PUPILS SHOULD NEVER:**

* access other people’s files without their permission;
* change or delete other people’s work/files without their permission;
* provide personal information such as telephone numbers and addresses when using the Internet;
* use electronic communication to arrange to meet anyone;
* use Social Media or equivalent while in school;
* bring in memory devices from home to use in school unless given permission by a member of staff;
* use any personal electronic devices they have their possession within school to access the internet or any messaging services unless permission has been given by a member of staff.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

**Student/Pupil Acceptable Use Agreement Form**

This form relates to the pupil acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

* I use the school systems and devices (both in and out of school)
* I use my own devices in the school (when allowed) e.g. mobile phones, USB devices, etc.
* I use my own equipment out of the school in a way that is related to me being a member of this school e.g. accessing school email, VLE, website etc.

Name of Pupil:

Class:

Signed:

Date:

# Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1)

#### 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 / tablets
* 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 / tablet

Signed (child):

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent / carer should be sufficient)

Signed (parent/guardian):

Date:

# Staff (and Volunteer) Acceptable Use Policy Agreement Template

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

#### 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 access to the internet and digital technologies 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 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology 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

**STAFF MEMBER: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**In line with Omagh County Primary School’s e-safety policy I understand:**

* I must not engage in any on-line activity that may compromise my professional responsibilities or bring the name of the school into disrepute;
* the school has the right to monitor my use of the school’s ICT systems, email and other digital communications;
* I will not search for, access, upload, download any materials which are inappropriate/illegal such as child sexual abuse images pornography, racist, sectarian or offensive material is forbidden;
* I must immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Principal or the school’s e-Safety co-ordinator;
* the use of school ICT systems for personal financial gain, gambling, political purposes or advertising is forbidden;
* I must not disclose my C2K username or password to anyone else, nor will I try to use anyone else’s C2K username and password;
* I will not use the school systems to access social media sites and I will not make friend requests to pupils or accept friend requests from pupils;
* 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 photographs/digital images;
* I must not access, copy, remove or otherwise alter any other user’s files, without their express permission; any activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
* when communicating electronically with others I should be professional, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;
* posting anonymous messages and forwarding chain letters is forbidden;
* the need to be cautious when opening attachments to emails, due to the risk of the attachment containing viruses or other harmful programmes;
* copyright of materials must be respected;
* that this Acceptable Use of the Internet Agreement 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 out of school and my use of personal equipment in school or in situations related to my employment by the school;
* 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 context of the school’s e-Safety policy;
* I will only use my personal mobile ICT devices as agreed in the school’s ‘e-Safety Policy’ and the school’s ‘Use of Mobile Phones and Related Technologies Policy’;
* I should immediately report any damage or faults involving equipment or software, however this may have happened;
* that if I have been granted enhanced Internet access to certain websites using the C2K system I must ensure that at all times no pupil has access to a computer on which I am logged on (unless under my supervision).
* when using the C2K system there is a log of my Internet searching history.

I understand that if I fail to comply with this Acceptable Internet Use Policy Agreement. I could be subject to disciplinary action, referred to the P.S.N.I. for further investigation and/or the procedures followed in line with the school’s Child Protection/Safeguarding Children Policy.

**I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.**

Signed:

Date:

# Parent / Guardian Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

* that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work.

**Permission Form**

Parent / Guardian’s Name:

Pupil Name:

As the parent / guardian of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son’s / daughter’s activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.

Parent/Guardian Signature:

Date:

# Responding to incidents of misuse – flow chart



# Record of reviewing devices/internet sites (responding to incidents of misuse)

Group:

Date:

Reason for investigation:

#### Details of first reviewing person

Name:

Position:

Signature:

#### Details of second reviewing person

Name:

Position:

Signature:

#### Name and location of computer used for review (for web sites)

|  |  |
| --- | --- |
| Web site(s) address/device | Reason for concern |
|  |  |
|  |  |
|  |  |

#### Conclusion and Action proposed or taken

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

## E-safety Incident Report Form

**Omagh County Primary School**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date happened:** | |  | |
| **Time:** | |  | |
| **Name of person reporting the incident:** | |  | |
| **If not reported how was the incident identified:** | | | |
| **Where did the incident occur?** | |  | |
| □ In school/service setting | | □Outside school/service setting | |
| **Who was involved in the incident?** | |  | |
| □ child/young person | | □staff member | |
| □ other (please specify) | |  | |
| **Type of incident** | |  | |
| □ bullying or harassment (cyber bullying) | | □deliberately bypassing security or access | |
| □ hacking or virus propagation | | □racist, sexist, homophobic religious hate material | |
| □ terrorist material | | □ drug/bomb making material | |
| □ child abuse images | | □ on-line gambling | |
| □ soft core pornographic material | | □hard-core pornographic material | |
| □other (please specify) | |  | |
| **Description of incident:** | |  | |
|  | | | |
| **Deliberate Access** | |  | |
| **Did the incident involve material being?** | |  | |
| □ created | □ viewed | □ printed | □ distributed |
| □ transmitted to others | | □ shown to others | |
| Could the incident be described as: | |  | |
| □ harassment | □ grooming | □ cyber bullying |  |
| **Accidental Access** | |  |  |
| Did the incident involve material being; | | |  |
| □ created | □ viewed | □ printed | □ distributed |
| □ transmitted to others | | □ shown to others | |
| **Action taken:** | |  | |
| **by staff** | |  | |
| □incident reported to principal | | □ advice sought from Safeguarding and Social Care | |
| □ referral made to Safeguarding and Social Care | | □ incident reported to police | |
| □ disciplinary action to be taken | | □ e-safety policy to be reviewed/amended | |
| **Please detail any specific action taken (e.g. removal of equipment):** | | | |
|  | | | |
| **by child** | |  | |
| □incident reported to principal | | □ advice sought from Safeguarding and Social Care | |
| □ referral made to Safeguarding and Social Care | | □ incident reported to police | |
| □ child’s parents/guardians informed | | □ disciplinary action to be taken | |
| □ child debriefed | | □ e-safety policy to be reviewed/amended | |
| **Outcome of incident/investigation** | |  | |
|  | |  | |

**Name of person filing report: …………………………………………………………………..**

**Signature: …………………………………………………………………..**

**Date: …………………………………………………………………..**