Harmony Primary School

E-Safety Policy

(2023)

Our Vision

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in E-safety can mean children are unaware of the unintended consequences of their on-line behaviour or actions. This policy highlights the need to educate pupils and the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to control their online experience.

'Our vision is to make the children at Harmony Primary School as safe and productive in the on-line world, both in school and outside of school, as they are in the real world with particular focus on protection against grooming, cyberbullying and becoming a positive e-citizen.'

Our policy and practice against this is clearly articulated in this E-Safety Policy.

DENI circular 2007/01 states:

"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."

Rationale

The Boards of Governors has a duty to:

- safeguard and promote the welfare of pupils; and
  (Article 17 of the Education and Libraries (Northern Ireland) Order 2003).

- determine the measures to be taken at a school to protect pupils from abuse
  (*Article 18 of the Education and Libraries (Northern Ireland) Order 2003).*

The rapidly changing nature of the Internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. The school has a duty of care to enable pupils to use on-line systems safely. This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. It covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

Introduction

Harmony Primary School understands that the Internet and other digital technologies are vast and powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. Harmony Primary school recognises that there are however many dangers with unsupervised and unguided use of the Internet and that we must provide pupils with opportunities to use the excellent resources available, along with developing the skills necessary to access, analyse and evaluate them.

eSafety is short for electronic safety and is about a school's ability to **protect and educate** its pupils and staff in their use of the internet through PC access and other electronic communications as well as having appropriate mechanisms in place to **respond** to, and **support** any incident where appropriate.

This document is largely based on DENI Circular 2007/1 '*Acceptable Use of the Internet and Digital Technologies in Schools*' and DENI Circular 2011/22 '*e-Safety Guidance*'. *It* should also be read in conjunction with other policies including those for ICT, bullying and Safeguarding.

This policy sets out what Harmony Primary School will do in order to protect pupils and staff and how it will guide and educate children in the wise and safe use of the Internet. As new technologies are developed, the school will respond quickly to any potential e-Safety threats posed by their use.

The policy has been drawn up by the school's e-safety team:

- Mrs Elaine Johnston (Principal)
- Mrs Claire Davidson (Designated Child Protection Teacher, Senior Leadership Team)
- Mr Robbie Best (ICT Co-ordinator)

The policy has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested. The policy and its implementation will be reviewed regularly.

eSafety within Harmony Primary School:

- is concerned with safeguarding children in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- 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;

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

Internet Access

Access to the Internet at Harmony Primary School is through a school broadband network connection provided by the Department of Education via C2K. The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

We believe that the proper use of this resource is consistent with our aims in:

- developing our children to their 'full potential'
- equipping them for 'life in our society'
- providing them with necessary 'life skills'
- permitting access to a range of materials which are consistent with our educational ethos

However, due to the unrestricted access to the Internet by a variety of groups or individuals there are materials which are unsuitable for school's viewing and may be racist, extremist, political, violent or pornographic in nature. Staff and pupils have access to the Internet through C2K servers which is a filtered service. This offers a protected environment for the users but no system is foolproof and therefore we feel it is appropriate to develop a set of guidelines which set out the parameters of acceptable use.

Code of Safe Practice

The Code of Safe Practice has been agreed with staff.

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. Staff and pupils are made aware that use of the school's ICT resources is a privilege which can be removed. The Code of Safe Practice for Harmony Primary School makes explicit to all users (staff and pupils) what is safe and acceptable and what is not.

The school has
(a) a Pupil Code of Practice (Appendix 1); and
(b) a Staff Code of Safe Practice (Appendix 2)

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, ipads and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, camera phones, PDAs) is subject to the same requirements as technology provided by the school.

Mr Best and the Senior Management Team will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

The Staff Code of Safe Practice highlights:

- Pupils accessing the Internet should on the whole be supervised by an adult at all times.
- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These will be displayed in classrooms and discussed with pupils.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to Mrs Davidson or Mr Best.
- In the interests of system security, staff passwords should only be shared with the network manager, Mr Best.
- Photographs of pupils should, where possible, be taken with school equipment and images stored on a centralised computer, accessible only to teaching staff or under supervision for pupil work.
- School systems may not be used for unauthorised commercial transactions.
- 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.

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. A Staff Safe Code of Conduct, which details sanctions, is signed by all staff.

<u>Code of Practice for pupils</u>

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 key measures have been adopted by Harmony Primary School to ensure our pupils do not access any inappropriate material:

- The school's e Safety Code of Practice for use of the Internet and other digital technologies (enclosed) is made explicit to all pupils and is displayed prominently;
- E-Safety guidelines are displayed prominently throughout the school;
- Pupils and their parents/carers are asked to sign the Code of Conduct sheets;
- Pupils, using the Internet, will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and supervised, where possible;
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group; eg through the use of QR codes;
- Pupils are educated in the safe and effective use of the Internet, through a number of selected websites and by participation in lessons on internet safety eg Safer Internet Day.

It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.
Use of mobile phones by pupils is not permitted on the school premises during school hours.

1.1 <u>Connectivity and Filtering</u>

C2K
Classroom 2000 (C2k) is responsible for the provision of an ICT managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.
The updated service in 2013-14 allowed for Improved Websense filtering which gave the school more flexible control. Customised filtering is managed by Mr Best (ICT Co-ordinator) who has received additional training for this responsibility and can further amend the local filtering policy to the needs and demands of the school. This enables the school to access more internet sites to enhance teaching and learning.

Internet use is monitored. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal devices are allowed, C2K filtering will be applied that is consistent with school practice.

Some of the safety services include:

- Providing all users with unique user names and passwords

- Tracking and recording all online activity using the unique user names and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses
- Filters access to web sites
- Use of 'securus' to monitor online activity

The school will take appropriate measures to safeguard non-C2K equipment against security breaches.

<u>Social networking and personal publishing</u>

The C2K system will block/filter access to social networking sites. Under the transformation internet filtering guidelines key staff will be given access for the purposes of updating Twitter. There are three internet filtering groups:

Internet Advanced
Internet Social Networking
Internet Streaming

All Staff will be given access to 'Internet Advanced'.
All Teaching staff will be given access to 'Internet Streaming' so that 'You Tube' can be used for Teaching purposes.
All children will be given access to 'Internet Streaming' so that they can view any 'You Tube' videos that Teachers have uploaded onto Fronter. Teachers will be extra vigilent.
Elaine Johnston will have access to social networking sites (Facebook and Seesaw).

Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location. Pupils and parents will be advised that the unmonitored use of social network spaces outside school is inappropriate for primary aged pupils.

<u>Managing filtering</u>

The school will work with C2K to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the ICT Coordinator. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Authorising Internet access

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a pupil's access be withdrawn.

For Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

2.2 Sanctions

We believe it is important that the school has a culture under which users understand and accept the need for e-Safety regulations and adopt positive behaviours, rather than one in which attitudes are determined solely by sanctions. Incidents of technology misuse which arise will be dealt with in accordance with the school's Behaviour Policy.

Minor school related incidents (whether in school or out of school) will be dealt with by Mr Best/Mrs Davidson and the Senior Management Team. This may result in parents being informed and a temporary ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's Safe Guarding Child Protection Policy.

Users will understand their responsibilities to report e-safety incidents. They will know and understand that there are clear systems for reporting abuse and understand that the processes must be followed rigorously. Incident reports will be logged by Mr Best for future auditing, monitoring, analysis and for identifying serious issues or patterns of incidents. This will allow the school to review and update e-Safety policy and practices.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately. The safeguarding team have an understanding of how to report issues online, should the need arise, including to CEOP.

3. Internet Safety Awareness

We believe that, alongside a written e-Safety Policy and 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, both inside school and outside school. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

3.1 Internet Safety Awareness for Pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety lessons take place throughout the school through a variety of curricular areas including P.D.M.U. using a range of online resources e.g. http://www.bbc.co.uk/cbbc/topics/stay-safe http://www.thinkuknow.co.uk/
- The whole school takes part in the Safer Internet Day.
- Key Stage 2 pupils participate in planned e-Safety education programmes during the year in partnership with Belfast City Council.
- Pupils are encouraged to enter e-Safety competitions and make posters.

Information is delivered and reinforced through school posters, the school website, newsletters and 'seesaw'.

Resources:

- *Child Exploitation and Online Protection (CEOP)* resources: a useful teaching tool looking at Internet safety
- *Childnet International* www.childnet.com has produced materials to support the teaching of e-Safety at Key Stage One and Two. They have materials for parents and staff too.

Other pupil resources available:

Superclubs, 360 e Safety Tool, *Signposts to Safety, KidSMART, Know IT All for Schools, ThinkUKnow*

3.2 Internet Safety Awareness for Staff/ Professional Development

Teachers are the first line of defence in e-Safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. E-Safety training is therefore an essential element of our staff induction and part of an on-going Continuous Professional Development programme. Through our e-Safety policy, the school can ensure that all reasonable actions are taken and measures put in place to protect all users.

All staff will be given the School e-Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

E-Safety training is linked with Safeguarding Training. Training needs are informed through audits. The induction programme for new staff includes e-Safety. The ICT Co-ordinator will keep informed and updated on issues relating to Internet Safety and attend courses when available. This training is then disseminated to all teaching staff, classroom assistants and supervisory assistants.

3.3 Internet Awareness for Governors

Mrs Johnston keeps governors updated on e-Safety and e-safety issues. The Board of Governors has appointed Elaine Conly as their representative on the school e-Safety team.

3.4 Internet Safety Awareness for Parents/ Carers and the Community

The Code of Safe Practice for pupils and Acceptable Use Agreement is sent home at the start of each school year for discussion with their child and parental signature. This e-Safety Policy and E-Safety materials are available on the school website. Internet safety leaflets for parents and carers are sent home annually. Parents/carers' attention is drawn to the school website and school newsletter where e-Safety messages are given. Parents are informed of the school's complaints policy which is on the school website. Parents are informed on how to report issues to the school.

3.5 Community Use of School ICT Resources

The school's ICT facilities are used as a community resource under the Extended Schools programme. Users are issued with separate usernames and passwords by C2K. The community may bring their own iPads/laptops and use these within the school's filtered policy. They must agree to the school's Use of the Internet policy before availing of the resources.

4. Health and Safety

In Harmony Primary we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and the ICT suite, which has been designed in accordance with health and safety guidelines and where pupils are supervised at all times. Guidance is issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

4.1 Risk Assessments

Life in the 21st century presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The school, to the best of its knowledge, has considered all new technologies wisely to ensure that it is fully aware of and can mitigate against the potential risks involved with their use. In so doing, pupils are informed of what to do if they come across inappropriate material or situations online.
The school cannot accept liability for the material accessed, or any consequences of Internet access.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

4.2 E-mail (if used)

Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.
Pupils must immediately tell a teacher if they receive offensive e-mail.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
The forwarding of chain letters is not permitted.

4.3 Use of Mobile Phones

We understand that some parents like their child to carry a mobile phone in-case of an emergency. Most mobile phones have internet connectivity. Pupils are permitted to have a phone in their school bag, but it must be handed to the teacher/office and be switched off during school hours. Please refer to the schools Mobile Phone Policy on the use of such.

Staff will not use mobile phones during lessons or formal school time. Staff should never give their telephone number to pupils for any reason and should not have a child's telephone number for any reason.

Staff must not take pictures or videos of pupils on their phones. The sending of abusive or inappropriate text messages is also forbidden.

The school has digital cameras and ipads, which are used for educational purposes, and photographs are deleted from these cameras after use.

4.4 Digital and Video Images

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area on the school network or a password protected internet storage facility, accessible only to teaching and support staff and are disposed of in accordance with the Data Protection Act. Parental permission is gained when publishing personal images on the website or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images (and in particular the risks attached).

4.5 Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available on The Health Protection Agency website.

4.6 Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

The school ensures all staff know and understand their obligations under the Personal Protection Act and comply with these to ensure the safe keeping of personal data, minimising the risk of loss or misuse of personal data.

4.7 Cloud Storage

Data and information is stored on the Cloud, meaning it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices.

4.8 Social Media

Social networking sites are a huge favourite with children, allowing them to stay in touch with friends over chat, meet new people with similar interests, and share photos and videos. Used appropriately, social networks are a great place for young people to demonstrate their creativity but as a school we recognise that care must be taken when making use of social media for teaching and learning especially since the lower age limit for most social networking sites is 13. The most popular social networks currently include Facebook, Instagram, YouTube, Twitter, Tumblr, Ask.fm and Snapchat. Sites aimed at younger children, like Club Penguin and Moshi Monsters, also have a social networking element

While social media technologies can offer much to schools and pupils, each one however brings its own unique issues and concerns. Each social media technology that is to be utilised will be risk assessed in the context of Harmony Primary.

Chatrooms, blogs and other social networking sites are blocked by the C2K filters and iPad wi-fi filters so pupils do not have access to them in the school environment. Such communication is maintained within the educational learning environment on the C2K system (Learning NI). However, we recognise that some of our pupils have access to such sites and therefore address the safe and responsible use of social media through our Internet Safety Education Programmes. We make staff, pupils and parents aware of the age requirements, benefits and risks associated with the use of social media and encourage responsible use outside school. Information and education is provided for parents on the school website, school newsletter and at parent and community internet safety meetings. Instances of pupil/staff cyber bullying will be regarded as serious offences and dealt with according to the school's discipline policy and child protection procedures.

4.9 Cyber Bullying

Cyberbullying, the deliberate targeting of someone to upset them, through the use of technology, is quickly outpacing the traditional forms of bullying. Preventing cyberbullying will not be easy, because of the fact it happens on the internet, children are subjected to cyberbullying at all times when they are online, including in their home.

Cyber bullying can work in the same way as bullying in the playground; the victim feels frightened and alone, while the bully tries to hide from being caught. Staff are made aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is considered within the schools overall Anti-Bullying policy and Pastoral Care Policy as well as the e-Safety Policy.

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 occurs 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.

It's important to remember that not all nasty messages posted online are defined as bullying. Sometimes, they are once-off. But when there is a prolonged campaign which appears to target one individual, then it becomes cyberbullying.

A lot of cyberbullying occurs when children lose sight of the consequences. Some don't think sending messages which they see as "just messing" or "joking" is bullying, and don't understand how it can hurt someone.

One of the most common reasons for cyberbullying is an attitude among bullies that they won't get caught. Internet anonymity empowers bullies and leaves them feeling like they cannot be traced. Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator. Pupils will be reminded that cyber-bullying can constitute a criminal offence.

While there is no specific legislation for cyber-bullying, the following covers 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

Pupils are encouraged to report incidents of cyber-bullying to their parents and the school. If appropriate, the PSNI may be informed to ensure the matter is properly addressed and behaviour ceases. The school will keep records of cyber-bullying incidents on SIMS to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

As a teacher or school staff member, it is your job to:-

- **Support**: Provide the person being bullied with support and reassurance. Tell them that they did the right thing by telling. Encourage the child to get help from parents, the school counsellor, principal or teachers. Ensure they know that there is support there for them
- **Evidence:** Help the child keep relevant evidence for investigations. This can be done by taking screenshots or printing web pages. Do not allow the deletion of phone messages
- **Inform:** Give the child advice for making sure it does not happen again. This can include changing passwords, contact details, blocking profiles on social networking sites or reporting abuse online
- **No Retaliation:** Ensure that the young person does not retaliate or reply to the messages
- **Privacy:** Encourage the child to keep personal information private on the internet
- **Investigation:** The cyberbullying claim needs to be investigated fully. Inform the school e-safety teacher or Designated child protection officer of the incident immediately. All records should be kept as part of the investigation.
- **Report:** Abuse on social networking sites or through text messaging needs to be reported to the websites and mobile phone service providers
- **Guidelines:** Ensure you and the children within your care are following the School's Acceptable Use, Anti-bullying and Behaviour and Disciplinary Policies.

Guidance for Staff

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

When asking to look at content on a student's personal device it is good practice to do so with 2 adults present and inform the parents as soon as possible.

Mobile Phones

- Ask the pupil to show you the mobile phone
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names

- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image
- Inform a member of the Senior Leadership team and pass them the information that you have
- If possible and with the pupil's agreement a screen capture image may be able to be sent to the staff's school email account, this should only be sent from the student's school email account. Use of other transfer systems such as SMS, Bluetooth, etc., to a personal phone or device of a staff member is not allowed.

Computers

- Ask the pupil to get up on-screen the material in question.
- Ask the pupil to save the material.
- Print off the offending material straight away.
- Make sure you have got all pages in the right order and that there are no omissions.
- Inform a member of the Senior Leadership team and pass them the information that you have.
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.
- If possible and with the student's agreement a screen capture image may be able to be sent to the staff's school email account, this should only be sent from the student's school email account.
- Use of other transfer systems such as SMS, Bluetooth etc. to a personal phone to device of the staff member is not allowed.

5. Other types of internet use

Spam &, Phishing and Viruses
Spam - unsolicited bulk messages, especially advertising.
Phishing - the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details.
Viruses/Adware/Malware - programs that may be harmful to your computer.

Online gaming

Online gaming means you can play in real time with people across the world through a computer, games console, tablet or smartphone connected to the internet. Games can offer children a world of adventure to immerse themselves in, but it's important to understand how children can stay safe and what games are appropriate for their age.

Some games contain 'avatars' which are an icon or figure representing a particular person.

Downloading & Viruses

Children delight in the freedom the internet gives them to download any song, film or TV programme they want. Most of the content children download is under copyright, meaning it belongs to the person, group or company that created it and payment is usually required. Downloading also exposes you to spyware and viruses.

Sexting

Sexting usually refers to sending and receiving rude messages or videos of:

- naked pictures
- 'underwear shots'
- any sexual texts, images or videos

Remember:

- There is no turning back once you press send.
- Even if you use apps like Snapchat the person can take a screen shot
- You risk being seen as someone you are not.

Online grooming

The internet is a highly interactive tool which can allow people to communicate with each other very easily, through internet chat programs and social networking sites and even mobile apps and games.

Paedophiles have been known to use this method to contact young people by disguising themselves as another young person. This can lead to gaining the trust of an individual and their friends. These false relationships based on lies can often pave way for exposure to upsetting images and online content and in some cases arranging a meeting in person.

Online grooming is the term used to describe inappropriate behaviour towards a young person, putting them at risk to a sexual offence.

Even if nothing dangerous does happen, knowing you may have had contact with somebody like this can be extremely upsetting.

Identity Theft

The more information you make available online, the greater the risk of identity theft. It can be very tempting to reply to an email or open an attachment or post information about yourself on social networking sites, but you should never do it.

Personal information includes your:

- email address
- phone number
- postal address
- any banking information
- photos of yourself

Cyber stalking

Harassment on the internet can be just as frightening as other forms of stalking.

- Women and girls are usually the victims of this kind of behaviour.
- They might be harassed by an ex-boyfriend or girlfriend who is upset about the end of their relationship, for example.
- It can also begin when a purely online friendship turns sour.
- It can even begin entirely at random, by one online stranger towards another.

6. School Website

The school website is used to celebrate pupils' work, promote the school and provide information. The website reflects the school's ethos. Information is accurate and well presented and personal security is not compromised. Parental permission, in writing, is sought for newly enrolled pupils to cover the use of photographs of pupils on the school website, app, in the local press and for displays etc within school. It is the parent’s responsibility to inform school of any changes in circumstances.

The ICT co-ordinator edits the website with assistance from the ICT team and Harmony Techies (pupils).

The following rules apply:

- The point of contact on the website is the school address, school e-mail and telephone number.
- Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully. Parents who prefer their child’s photographs do not appear on the school website is respected.
- Pupils' full names will not be used in association with photographs.
- The Principal will take overall editorial responsibility and ensure content is accurate and appropriate.

- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

7. Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters and the school brochure. Parents will all receive a copy of the policy for their own information.

8. Handling e-safety complaints

For safe practice to be a reality, pupils, teachers and parents must know how to submit a complaint. The Complaints Policy is available on the school website and in paper form from the school office. If parents, pupils or members of the public have concerns they should:

1. Discuss their concerns with the member of staff most directly involved and, if not satisfied;
2. Discuss their concerns with a senior member of staff and, if not satisfied;
3. Discuss their concerns with the Head teacher. If the Head teacher considers she can do no more to resolve
the complaint it will be stated explicitly that the complainant can write to the Chair of Governors if not satisfied.
Complainants are encouraged to state what actions they feel might resolve the problem at any stage.

Prompt action will be taken if a complaint is made. A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's Disciplinary Policy.

Complaints of Internet misuse will be dealt with by a senior member of staff.
Any complaint about staff misuse must be referred to the head teacher.
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
Pupils and parents will be informed of the complaints procedure.

9. Monitoring and Self Evaluation

This policy will be reviewed and amended in light of evidence provided by monitoring, updated technologies or new EA Guidance.

E-safety lessons will include teaching children that:-

Personal Information is Personal

Pupils learn to never give out personal details such as; name, address, date of birth and school.

They are taught that user names and passwords should not contain personal information

We should treat others online as we do in the real world

Pupils learn that online bullying and harassment are potential problems that can have a serious effect on children. They are aware that causing upset or harm online will follow the same sanctions as outlined in our behaviour policy

Strangers Online are still strangers

Pupils learn to recognise that friends are people we know and see regularly as part of our everyday lives. Online "friends" are strangers and invitations to meet them in the real world should be reported.

We should monitor and evaluate what we see and do

Pupils learn to monitor and evaluate everything they see, read and do in order to refine their own publishing and communications with others via the Internet, ensuring it is of an acceptable standard.

What to do if something isn't right

Pupils learn that if they know or feel something isn't right that they should speak to, or contact an adult immediately.

a. Acceptable Internet Use Policy for Staff

All school equipment is owned by the school, and may be used by pupils to further their education and by 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 pupils, the staff and the school. To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's E-safety Policy for further information and clarification. Specifically:

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my network area and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report incidents of concern regarding children's safety to the school's designated Child Protection Co-ordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote E-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with Acceptable Use Policy.

Signed: Date:

b. ICT Code of Practice Letter to parents

ICT Code of Practice

Dear Parent/Carer,

As part of our curriculum we encourage pupils to make use of educational resources available on the Internet. Access to the Internet enables pupils to conduct research and obtain high quality educational resources from libraries, museums, galleries and other information sources from around the world.

To guard against accidental access to materials which are inappropriate in school our access to the Internet is provided by the Department of Education via C2K. However, it is not possible to provide a 100% assurance that pupils might not accidentally come across material which would be inappropriate.

Therefore, before they access the Internet we would like all pupils to discuss the ICT Code of Practice with their parents/carers and then return the signed form to your child's class teacher.

We believe that the educational benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, far outweigh the potential disadvantages.

During lesson time teachers will guide pupils toward specific materials and educational resources. Where pupils are given permission to access the Internet outside lessons they must agree to access only those sites that are appropriate for use in school and use the e-learning resources appropriately.

Yours sincerely

****

Pupil: Date: Year Group:

My parents and I have read the ICT Code of Practice and I agree to follow it.

Pupil Signature Date

Parent:

As parent or carer, I have read, discussed and explained the ICT Code of Practice to my son/daughter. I understand that if he/she fails to follow this code, his/her individual access may be withdrawn and I will be informed.

Parent/Carer Signature Date

c. Children's ICT Code of Practice

The school has computers and tablet devices with access to the Internet to support our learning. These rules will help keep us safe and help us be fair to others.

Using the Computers:

- I will respect all computer equipment and will report any damage or faults.
- I will only access the school computer system with my own login and password, which I will keep secret.
- I will not change any settings on the computers without my teacher’s permission.
- I will not delete anything from the computer without my teacher’s permission.
- I will not access or change other people's work.
- I will only bring in memory sticks or CD ROMs from outside school to use on the school computers, if I have been asked.
- I understand that my teacher can look at my computer files at any time.
- I will never give out personal information or passwords.

Using Mobile Technology:

- I will only use the iPads and other tablet devices when I have been given permission to by my teacher.
- I will use the tablet responsibly and make sure that it is returned after I have used it.
- I will not use any Apps that I have not been given permission to use.
- I will not take photographs or film children or adults without their permission.

Using the Internet:

- I will ask permission before using the Internet.
- I will be aware of “stranger danger”, when working online.
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and me.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will not complete and send online forms without permission from my teacher.
- I will not give my full name, my home address or telephone number when using the Internet.
- I will learn about copyright laws and make sure I acknowledge resources
- I will not upload or download images, music or videos without permission
- I will check that the information that I access on the internet is accurate, as I understand that the internet may not be truthful and may mislead me.

Using E-mail:

- I will ask permission before sending an e-mail.
- I will only e-mail people I know, or my teacher has approved.
- I will not use or open email, unless I know and trust the person or organisation.
- I will immediately report any unpleasant messages or material sent to me because this will help protect other pupils and me.
- I understand that e-mail messages I receive or send may be read by others.

- The messages I send will be polite and responsible.
- I will only send an e-mail when it has been checked by a teacher.
- I will not give my full name, my home address or telephone number.
- I will not use e-mail to arrange to meet someone outside school hours.

Cyber Bullying

- I will be polite when I communicate with others
- I know not to do online what I wouldn't do offline like in the playground
- I will not use inappropriate language or make unkind comments
- I appreciate others may have different opinions
- I will not upload or spread images of anyone

Mobile Phones

- I know that mobile phones are not allowed to be used during the school day and are advised to be left at home.
- If consent has been given then mobile phones are switched off / silent and kept in a designated place or in the office at all times during the school day.
- Permission must be given by the principal if I can use a mobile phone in school or take it on a school visit.
- I know not to use text, voice messages, take images or use any internet connection to bully, upset or shock anyone in and out of school.
- I know that no images or videos should be taken on any mobile phones or personally-owned mobile devices without the consent of the person or people it involves.
- I know that the school is not responsible for any loss or damage to my mobile phone or any device I bring onto the school site.
- I understand that the school have a right to confiscate, search and keep any evidence on any mobile devices I bring into school.
- I know that I should protect my phone number by only giving them to trusted friends and family.

Outside of the School Community

- I understand that this agreement is for in and outside the school
- I know there will be consequences if I am involved in incidents of inappropriate behaviour covered in this agreement

All pupils need to sign these rules on the form provided and/or in class with a teacher at the start of each new academic year. This shows that they have read, understood and agree to the Pupil ICT Code of Practice.

Pupil Signature: ______________________________________

Today's Date: ______________________________________

d. Pupil i-pad agreement

Harmony Primary School

ICT Code of Practice Agreement for Pupils – iPad usage

The school has iPads to enhance learning. We can access the internet on these ipads and will follow the internet Code of Practice.

I will take good care of any iPad I am using.

I will never leave the iPad unattended.

I will keep food and drinks away from my iPad since they may cause damage to the device.

I will not disassemble any part of an iPad or attempt any repairs.

I will protect any iPad I am using by only carrying it whilst it is in a case.

I will use the iPad in ways that are appropriate.

I will only photograph people with their permission.

I will only use the camera or the microphone when my teacher tells me to.

I will never share any images or movies of people in a public space on the Internet, unless I am asked to do so by my Teacher.

I will access the Internet safely on the iPad.

e. ANTI-CYBERBULLYING POLICY

Harmony Primary School is committed to teaching children the knowledge and skills to be able to use ICT effectively, safely and responsibly in order to ensure that children are safe and feel safe from bullying, harassment and discrimination.

Cyber bullying Defined:

Cyber bullying can be defined as the deliberate targeting of someone to upset them, through the use of technology. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.

Aims of Policy:

- To ensure that pupils, staff and parents understand what cyber bullying is and how it can be combated.
- To ensure that practices and procedures are agreed to prevent incidents of cyber bullying.
- To ensure that reported incidents of cyber bullying are dealt with effectively and quickly.

Understanding Cyber bullying:

- Cyber bullying is the use of ICT (usually a mobile phone and or the Internet) to abuse another person.
- It can take place anywhere and involve many people.
- Anybody can be targeted including pupils and school staff.
- It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorised publication of private information or images etc.

Procedures to Prevent Cyber bullying:

- Staff, pupils, parents and governors to be made aware of issues surrounding cyber bullying.
- Pupils and parents will be urged to report all incidents of cyber bullying to the school.
- Staff training will assist in learning about current technologies.
- Pupils will be involved in developing and communicating this policy.
- Pupils will learn about cyber bullying through PDMU, assemblies, Anti-bullying Week activities and other curriculum projects.
- Pupils will sign an ICT Code of Practice agreement form.
- Parents will be provided with information and advice on how to combat cyber bullying. This will be displayed on the parent noticeboard and the e-safety page on the school website.
- Parents will be expected to sign an ICT Code of Practice agreement form and to discuss its meaning with their children.
- Pupils, parents and staff will be involved in reviewing and revising this policy and school procedure.
- All reports of cyber bullying will be investigated, recorded, stored in the Headteacher's office and monitored regularly.
- The Education Authority can provide support and assistance in dealing with incidents of cyber bullying and can be contacted by staff and parents. The police will be contacted in cases of actual or suspected illegal content.

f. Start of year – class Internet Safety Check discussion

It is good practice to discuss these points with pupils at the start of the school year, the start of a project requiring Internet use, or if revision of Acceptable Internet Use is necessary.

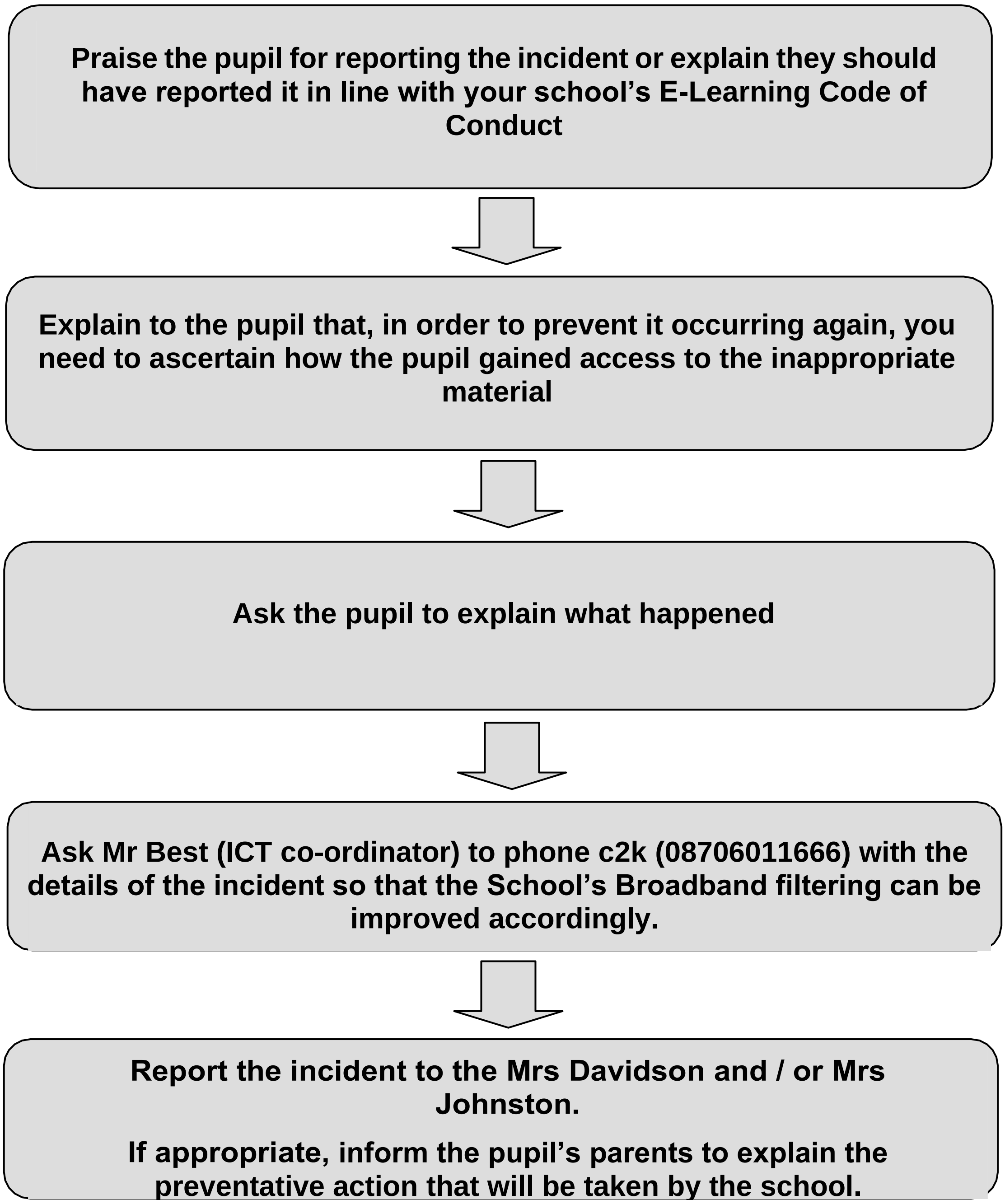
- **Only use the Internet when there is a teacher or other adult present to supervise or when you have been given specific permission.**
- **Only use your own login name and password. Never use another person's details.**
- **Never give out your address, phone number or arrange to meet someone over the Internet.**
- **All e-mails, messages in forums and text messages should be polite, appropriate and sensible. Do not send any e-mail or text message which could cause upset.**
- **If you receive a rude or offensive message you must report it to a teacher immediately. Do not pass on rude or offensive messages. What may seem funny to you may not be funny to someone else.**
- **If you see anything offensive or if you feel uncomfortable about anything, report it to your teacher or to an appropriate member of staff.**
- **Be aware that the school may check your computer files and monitor the Internet sites you visit.**
- **Ask an adult if you are unsure that a web source is reliable and information you are going to use is accurate.**
- **You and your parents should have signed the school Internet Agreement. You will be breaking that Agreement if you deliberately break these rules. This could result in you losing your Internet access at school.**

Draw pupil's attention to the poster on the wall in the classroom regarding sensible conduct whilst using the Internet. They can refer to this anytime they need a reminder.

g. Guidelines on Inappropriate Internet Access

Whilst using the Internet during school hours, a pupil **accidentally** finds a website displaying inappropriate material. What should you do?

Use this step-by-step guide to help you follow the correct procedure for reporting inappropriate materials from the Internet.



Praise the pupil for reporting the incident or explain they should have reported it in line with your school's E-Learning Code of Conduct

Explain to the pupil that, in order to prevent it occurring again, you need to ascertain how the pupil gained access to the inappropriate material

Ask the pupil to explain what happened

Ask Mr Best (ICT co-ordinator) to phone c2k (08706011666) with the details of the incident so that the School's Broadband filtering can be improved accordingly.

Report the incident to the Mrs Davidson and / or Mrs Johnston.

If appropriate, inform the pupil's parents to explain the preventative action that will be taken by the school.

h. E-Safety Incident Recording Form

Please record sufficient detail to enable the monitoring of incidents.

Type of Incident:	✓	**System Location:**	✓
Bullying (cyber bullying)		Computer Suite	
Grooming		Classroom	
Sharing inappropriate messages		Corridor	
Sending inappropriate images		Outside school premises	
Hacking or virus spreading		Other (record in **description** below)	
Accessing racist, sexual or homophobic material			
Sharing racist, sexual or homophobic material		**Device accessed on:**	✓
Accessing religious hate material		Laptop	
Sharing religious hate material		Desktop computer	
Accessing pornographic material		iPad/Tablet	
Sharing pornographic material		Mobile phone	
Other (record in **description** below)		Other (record in **description** below)	

Date:	**Time:**
Description of what happened:	

Accidental Access:	**Deliberate Access:**

Child/ren Involved:	Year	SEN	Disability	Ethnic Group	Involvement in Incident

Member of staff recording the incident:
Role:

Other staff involved:
Role:

Action Taken:

If appropriate:	Yes ✓	No ✓
Have you copied this Incident Form for the class teacher?		
Have you had contact with the parents/carers of all children involved? If Yes, by phone / letter? Date of contact:		
Are any other agencies involved? If Yes, which agencies? If Yes, and the incident was prejudice-motivated, consult Education Authority as to whether a Hate Crime report is appropriate.		
Does the incident require Police/CEOP involvement?		

Signed:

Name:

Date:

Status:	✓
Resolved	
Unresolved	
Further intervention needed	
C2k informed (if appropriate)	

File THREE Copies (tick when actioned)	**Headteacher**	**Child's File**	**E-safety File**

Details of any subsequent actions or follow-up:
(Include dates)

Figure 3

iPad Acceptable Use Policy Harmony Primary School

The policies, procedures and information within this document applies to all iPads or any other IT handheld device used in School.

Users Responsibilities

Users must use protective covers/cases for their iPad.

The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop or place heavy objects (books, laptops, etc.) on top of the iPad.

Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.

Do not subject the iPad to extreme heat or cold.

Do not store or leave unattended in vehicles.

Users may not photograph any other person, without that persons' consent.

The iPad is subject to routine monitoring by Harmony Primary School. Devices must be surrendered immediately upon request by any member of staff.

Users in breach of the Responsible Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Harmony Primary School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

Safeguarding and Maintaining as an Academic Tool.

iPad batteries are required to be charged and be ready to use in school.

Items deleted from the iPad cannot be recovered.

Memory space is limited. Academic content takes precedence over personal files and apps.

The whereabouts of the iPad should be known at all times.

It is a user's responsibility to keep their iPad safe and secure.

iPads belonging to other users are not to be tampered within any manner.

If an iPad is found unattended, it should be given to the nearest member of staff.

Lost, Damaged or Stolen iPad

If the iPad is lost, stolen, or damaged, the ICT Co-ordinator and Head Teacher must be notified immediately.

Prohibited Uses (not exclusive):

Accessing Inappropriate Materials – All material on the iPad must adhere to the ICT Responsible Use Policy. Users are not allow to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.

Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.

Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation.

Images of other people may only be made with the permission of those in the photograph.

Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of the Teacher or in the case of staff use; a member of the Senior Leadership team.

Use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.

Misuse of Passwords, Codes or other Unauthorised Access: Users are encouraged to set a passcode on their iPad to prevent other users from misusing it.

Anything downloaded from the Apple store using a personal Apple ID will be visible even when signed-in using your school Apple ID. The same goes for photographs.

Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.

Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.

Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.

Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.

Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.

Users should be aware of and abide by the guidelines set out by the School eSafety policy.

Harmony Primary School reserves the right to confiscate and search an iPad to ensure compliance with this Responsible Use Policy.

Adult Users must read and sign below:

I have read, understand and agree to abide by the terms of the iPad Acceptable Use Policy.
Signatures:

Figure 4

Using Pupil Images

TEACHER SECTION ONLY

I have read and understood the conditions for using images as detailed below.

Signed (Class Teacher): ______________________________________

Date: ______________________________

Print name: ____

Conditions of Use

1. This form is valid for 1 academic year from the date of signing. Your consent will automatically expire after this time.
2. We will not include details or full names (which means first name and surname) of any person in an image on the website, or in printed publications, without good reason and only with your express consent.
3. We will not include personal e-mail or postal addresses, or telephone numbers on our website or in printed publications.
4. We may use group images with very general labels, such as ‘Choir’ or ‘making Christmas decorations’.
5. We will only use images of pupils who are suitably dressed; to reduce the risk of such images being used inappropriately e.g. we will not publish material from swimming lessons.

Figure 5

YouTube – Teacher Responsibilities

As YouTube (www.youtube.com) is now available to teachers in school it is important that we are all aware of how to use this website correctly.

Teachers must be aware of the following:

There is inappropriate content on this website and we must be careful when navigating through the website and searching for clips. Perhaps this should be done out of the sight of children,

Teachers must watch any clips in their entirety before showing them to their class so that they know exactly what is on it.

Teachers must judge the content of the clip to be appropriate to the age level watching it.

It is the teachers own personal responsibility to use this website safely and appropriately.

Can all teachers sign and date below as evidence of reading and understanding all the points above.

Thanks,

Mrs E Johnston (Principal) and Mr R Best (ICT Coordinator)

SIGNATURE	DATE

SIGNATURE	DATE