# **Churchill Primary School**

# **Online Safety Policy**

# **And**

# **Acceptable Use Agreement**



# **Updated June 2020**

# **Introduction**

# Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

# Websites

# Learning Platforms and Virtual Learning Environments

# Email and Instant Messaging

# Chat Rooms and Social Networking

# Blogs and Wikis

# Podcasting

# Video Broadcasting

# Music Downloading

# Gaming

# Mobile/Smart phones with text, video and/or web functionality

# Other mobile devices e.g. ipad/ipod/tablet with web functionality

# Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

# In ***Churchill Primary School*** we understand the responsibility to educate our pupils in Online Safety issues. We aim to teach appropriate behaviours and critical thinking to enable pupils to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

**What is Online Safety?**

“*Online safety means acting and staying safe when using digital technologies. It is wider than simply internet technology and includes electronic communication via text messages, social environments and apps, and using games consoles through any digital device. In all cases, in schools and elsewhere, it is a paramount concern.”* DENI Safeguarding and Child Protection in Schools: A guide for Schools (Sep 2019)

“*Online safety is about using digital devices in a smart but safe way. It means educating children and young people to act responsibly and keep themselves safe in the digital world*.” C2K Support Materials on Fronter (May 2017)

This Online Safety Policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. Online safety covers not only Internet technologies but also electronic communications via mobile phones, ipads, games consoles and wireless technology. Effective online safety plays a crucial role in highlighting the impact of behaviour when engaging in online technologies and educating children and young people about how to act appropriately and stay safe.

Online safety is an integral component of our safeguarding procedures and this policy applies to all members of Churchill Primary School community; pupils, teachers, peripatetic staff, volunteers, parents or carers and visitors who have access to and are users of our school ICT systems, both in and out of the school.

In Churchill Primary School, online safety:

* is concerned with safeguarding children and young people in the digital world;
* emphasises learning to understand and use new technologies in a positive way;
* is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
* is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
* is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.
* Enables pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online safely.

Young people’s extensive use of technology and the rapidly changing nature of the internet and new technologies means that online safety is an ever growing and changing area of interest and concern. The school’s online safety policy aims to reflect this by keeping abreast of the changes taking place. Churchill Primary School has a duty of care to enable pupils to use on-line systems safely.

Churchill Primary School’s Online Safety Policy operates in conjunction with other school policies including Safeguarding/ Child Protection, Positive Behaviour, Anti-Bullying and Acceptable Use. We deliver a planned and progressive online safety curriculum to enable children to develop a clear understanding of online safety issues and to explore what a positive digital footprint might look like for themselves. ICT is a compulsory cross-curricular element of the revised curriculum and the school will ensure acquisition and development by pupils of these skills.

**What are the risks?**

Four categories of risks have been identified (Safeguarding Board NI 2014)

* **Content risks:** the child or young person is exposed to harmful material.
* **Contact risks**: the child or young person participates in adult initiated/child initiated online activity.
* **Conduct risks**: the child or young person is a perpetrator or victim in peer‑to‑peer exchange.
* **Commercial risks:** the child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs.

This policy has been created in line with:

* **DENI Circular 2016/27** “Online Safety”
* **DENI Circular 2016/26** “Effective Educational Uses of Mobile Digital Devices”
* 360 Degree Online Safety Self-Review Tool for Schools (April 2020) https://360safe.org.uk/Overview
* DENI “**Safeguarding and Child Protection in Schools**: A Guide for Schools” (Sep 2019)

**Σ**

**A consistent whole school approach.**

Churchill Primary School adopts a consistent whole school approach to online safety. In Churchill Primary School:

* Safeguarding including Online Safety is a key priority of all teaching and non-teaching staff, volunteers, visitors and the Board of Governors.
* All teaching and non-teaching staff can recognise and are aware of Online Safety issues.
* Online Safety Training of teaching and non-teaching staff is appropriate and organised.
* Online safety messages are integrated across the curriculum for pupils in all Key Stages.
* Online safety messages are distributed amongst pupils, staff, parents or carers and the wider community.
* Knowledge is shared amongst staff and there are good capacity building opportunities.
* There is on-going monitoring and evaluation of policy and practice.

**Professional Development for Staff**

All teaching and non-teaching staff of Churchill Primary School are familiar with our Online Safety Policy. Staff are trained to recognise and to be aware of online safety risks and on how to report or act on these. Staff training on online safety risks forms part of Child Protection Training during the Baker Days in August and other relevant times as need arises.

* Staff have read, understood and signed the school’s Staff Acceptable Use of the Internet Agreement.
* Staff report any online safety incident to the ICT Co-ordinator and the appropriate records are kept in our online safety register. If it is a safeguarding or child protection issue this will be reported to the Designated Teacher or the Deputy Designated Teacher.
* Circulars relating to online safety are emailed to all staff for their information.
* Staff share good practice in relation to online safety through curriculum meetings.
* We recognise that some members of staff are more confident and competent users of digital technology and they are encouraged to share their good practice e.g. sharing of websites which promote online safety
* Internet use should be planned, task orientated and educational within a regulated and managed environment. It is best practice that pupils should be guided to sites checked as suitable for their use.
* Supervision is a key strategy. Pupils should have an adult present when accessing the internet and computers need to be positioned for adults to see the content on the screen.
* Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
* Staff discuss with pupils the rules for responsible internet use as pupils need to be taught how to be internet wise and learn how to recognise and avoid potential risks.
* Age appropriate User Agreements and internet safety rules, reminders and the procedures for reporting an internet safety issue or concern are displayed in the ICT area of each classroom.

**School Websites and Use of Images**

It is our schools’ policy that names of children are not displayed or published alongside photographs to identify a child on the school website or social media accounts. When displaying photographs of certificate or prize winners, photographs are edited to blank the names in line with GDPR.

Parental permission is sought at the start of the academic year to allow photographs or examples of pupils’ work to be published on a website, school Facebook page, in the press or in other instances in the public domain. Teachers will be informed by the school office of any children in their class who do not have parental permission to have their photograph taken.

**Staff Use of the School’s Internet Service**

* The school wishes to encourage the use of e-mail and internet by staff in support of their work, noting that all use of these facilities should be appropriate to the work, standards and ethos of the school.
* The use of the school’s internet and e-mail systems is not provided as a right to any of their users. They may be withdrawn from any user, adult or pupil who does not conform to this Acceptable Use and that of C2K.
* The school is responsible for authorising any user of its internet or e-mail facilities, and should monitor and police their use.
* Any member of staff who commits a serious offence in the use of the school’s internet service may be subject to the school’s staff disciplinary procedures.
* Illegal activity using the school’s internet service will be reported to the police as necessary.
* Never pass on, make obvious or leave in an insecure place any passwords associated with using the internet, e-mail and C2K computer system.
* Never provide personal details or contact details of your own, or any other person, to internet sites including weblogs, forums or chat rooms. Exceptions should be checked with our ICT Coordinator or Principal. At all times comply with the Data Protection Act.
* If you see any unacceptable site or material as a result of an innocent internet query, unsolicited pop-up window or in any other way, report it immediately to the ICT Co-ordinator or Principal.
* Staff or approved adult school users should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet.
* Staff using a school computer, ipad or other device off the school site, at home or elsewhere, will still have to abide by the school and C2K internet Acceptable Use Agreement .
* Never upload an image of pupils or staff without their permission and always ensure that it meets with the ethos of our school and the principles behind the acceptable use agreement.
* Staff will at all times work to maximise the safety of pupils within their care in their use of the internet. If they feel they are working with an aspect of ICT beyond their knowledge then they should seek support from a colleague or the ICT coordinator before using with pupils.
* Colleagues will be aware of the ethos and standards of the school and will not access any internet material, or work with the internet, in any way that infringes or offends these.
* Online safety training and the signing of the acceptable use agreement is an essential element of staff induction and regular training and updates are part of an on-going Continuous Professional Development programme.
* Teachers are the first line of defence in online safety; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Incidents can vary from the prank or unconsidered action to illegal activity.
* Staff at Churchill PS will avail of training and support to determine what action is appropriate including when to report an incident of concern to the school’s ICT Co-Ordinator or the Designated Teacher for Safeguarding and Principal.
* Additional support and advice will be sought from C2k, Social Services or the PSNI if required.
* The school will ensure that all reasonable actions are taken and measures put in place to protect all users.

**Education of Pupils**

All children and young people have a right to be educated and at Churchill Primary School we recognise our responsibility to ensure that there is a reduced risk of pupils accessing harmful and inappropriate digital content.

Through our preventative curriculum we aim to be energetic in teaching pupils how to act responsibly and keep themselves safe in a digital world and, as a result, pupils should have a clear understanding of online safety issues and be able to demonstrate what a positive digital footprint might look like for themselves.

We have developed a progressive scheme of online safety lessons for all classes from P1-P7 which explore age appropriate content and issues such as pop ups, passwords, social media, gaming, cyber bullying etc.

Alongside online safety assemblies we plan five online safety weeks throughout the year where online safety is the focus of our PDMU sessions. We have annual visits by PSNI to talk to all classes about staying safe online.

**Resources**

* We adopt a preventative approach to online safety.
* We actively promote online safety messages for pupils on how to stay safe, how to protect themselves online and how to take responsibility for their own and others’ safety.
* Internet Safety posters from websites such as www.kidsmart.org.uk are displayed around the school to help reinforce safety messages for pupils.
* Materials from outside agencies are also distributed to pupils for use in school or at home with their parents.
* Online safety lessons are integrated by staff across the curriculum for pupils in all Key Stages.
* Safer Internet Day is celebrated through assemblies and class activities.
* Further learning opportunities are incorporated into ICT lessons through the use of C2K Newsdesk.
* Pupils understand the importance of reporting abuse, misuse or access to inappropriate materials and know the procedures to follow.
* The Key Stage 2 class visit RADAR in which online safety is highlighted.

There are clearly defined procedures for reporting and dealing with incidents surrounding breaches in the school’s online safety guidelines and children are aware of how to report an issue or concern.

See Appendix 2: Resources

Appendix 3: How to report an incident.

**Involvement of parents and carers.**

Parents or carers play a crucial role in ensuring that their children understand the need to use the internet and digital devices safely and in an appropriate way.

Churchill PS parents or carers are helped to understand and follow the school’s Online Safety Policy. They and their children annually sign our Pupil Acceptable Use of the Internet Digital Devices.

We believe that parents and carers have an essential role in the education of their children and in the monitoring of their on-line behaviours. Parents and carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure how to respond. The school will therefore help provide information and awareness to parents or carers through class assemblies and via the school website or Seesaw.

**Risk Assessments**

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become “Internet-wise” and ultimately good “digital citizens”.

The school has performed a risk assessment on the technologies within the school to ensure that they are fully aware of and can limit the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessment will inform the teaching and learning, develop best practice and be referenced in the school’s Acceptable Use Agreement

See Appendix 3: Risk Assessment

**RAMP**

If any concerns arise over a child’s search history relating to sexual content or sexually inappropriate language or behaviour a RAMP (Risk Assessment Management Plan) will be completed and a referral will be made to the Child Protection Intervention Team.

**Cyber Bullying and the link to Anti Bullying Policy**

Staff should be 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 school’s Anti -Bullying policy and pastoral services as well as the online safety policy.

Appendix 4: Children’s poster for reporting online safety issue/ concern

Care should be taken when making use of social media for teaching and learning (See CPS Social Media Policy) In Churchill PS we do not endorse the use of social media for teaching and learning as although it can offer much to schools and pupils, it also brings its own unique issues and concerns.

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:

* 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 will be 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.

Churchill PS will also keep good records of cyber-bullying incidents, as outlined in the Anti-Bullying Policy, to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

**Service Providers**

**C2K Services**

Churchill Primary School uses the C2K system on all desktop computers and laptops, which is monitored. Security reports can be accessed by the school principal.

The C2k services put in place have been designed with a clear focus on online safety. The main online safety elements that the school needs to be mindful of in planning and implementation are outlined in Appendix 1.

C2k provides every pupil and member of staff with a unique username to access C2k services. Authenticated users are granted access to C2k’s filtered internet service. User activity is logged and reports of usage are available to nominated staff within a school. Where a school suspects inappropriate use of the internet, the facility to remove access for a user exists.

The C2k wireless service enables schools to introduce other technologies to support teaching and learning. These new technologies will be examined for educational benefit and a risk assessment carried out before they are purchased or used in classrooms.

The school online safety Policy will be updated when new technologies are introduced and after a risk assessment has been completed.

**Ipads and other digital technologies**

Pupils and staff in Churchill Primary School use ipads throughout their learning. We want pupils to have opportunities to avail of all the positive benefits that come from learning, exploring and connecting with each other online through means and equipment relevant to their everyday lives.

Access to the internet through these devices is through a line operated through the C2k filtered Network.

**Email Security**

All staff and pupils are encouraged to use their C2k email system. The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

Staff and pupils should not use non C2k emails accounts in school.

**Internet Security**

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.

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

**Acceptable Use Agreement**

Internet access, monitoring and security measures will be utilised by the school where appropriate and these are highlighted in the school Acceptable Use Agreement. Staff and pupils need to understand that the use of the school’s information technology resources is a privilege which can be removed.

# Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school’s e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.

# All parents will be asked to sign the Acceptable Use Agreement for pupils annually giving consent for their child to use the Internet in school by following the school’s e-Safety rules and within the constraints detailed in the school’s e-Safety policy. This document will be countersigned by pupils in P3-7 also.

# All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

### See Appendix 5: Acceptable Use

**Communication of the school’s Online Safety Policy**

Churchill Primary School will introduce and share this policy with all users including teachers, parents, Governors, support staff and pupils.

There is an area of the website dedicated to online safety keeping all stakeholders informed and up to date with legislation/ guidance and resources.

**Appendix 1: C2k Safety Elements which need to be prepared and planned for during 2020/21**

|  |  |
| --- | --- |
| Internet Filtering | Improved Websense filtering gives schools the flexibility to control and develop their own Internet Filtering Policy. Individual schools may now select to fully delegate management of their filtering policy to a nominated member of staff by signing up to C2k delegated filtering access. This nominated user will receive additional training for this responsibility and can further amend the local filtering policy to the needs and demands of the school. This is in direct response to feedback from schools, who wish to access more internet sites to enhance teaching and learning. However there are a number of agreed locked down sites that can never be overridden by the local school policy. |
| Meru Wireless | Meru Wi-Fi provides increased wireless coverage and improved speed. Meru supports multiple devices and school controlled secure guest access and allows schools to plan for and implement a further purchase by the school or/and a ‘Bring Your Own Device’ policy. |
| Cloud Storage | Data and information will be stored on the Cloud in the new service and no longer in the school itself. This means it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices. |
| Granular Controls  Ipads and other mobile devices | Through the management console, each school C2k Manager will be able to control access to the internet and services to named individuals and groups of users based on their role in the school, their age, courses studied or to support individual needs.  Children and staff are aware of the acceptable use of the internet and digital technologies and have signed contracts to agree to the terms set by the school. They are aware of how to report an incident or concern and all access to the internet is filtered and monitored closely. |

**Appendix : 2 Resources**

www.360safe.org.uk

Child Exploitation and Online Protection (CEOP) Online resources

www.thinkuknow.co.uk

[www.childnet.com](http://www.childnet.com)

net-aware.org.uk

**Appendix 3: Risk Assessment for online safety**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ACTIVITY** | **HAZARD** | **WHO MAY BE AT RISK** | **CONTROLS REQUIRED** | **FURTHER CONSIDERATIONS** |
| Using the Internet | Accessing of unsuitable content. | Pupils  Teachers  Support staff | C2K Network Filtering Solution | Pupils taught about Internet safety |
| Use of email | Sending and receiving messages with inappropriate content. | Pupils  Teachers  Support staff | C2K Network Filtering Solution | Pupils taught about sending and receiving inappropriate content |
| Communication via Mobile Phones | Sending and receiving messages/photos with inappropriate content. | Pupils  Teachers  Support staff | … Policy states that pupil mobile phones should be turned off in school.  Only approved school cameras/iPads to be used in school and on educational visits | Pupils taught about sending and receiving inappropriate content |
| Use of Cameras/ camera phones/ recording devices | Sending photos with inappropriate content. | Pupils  Teachers  Support staff | Only approved school cameras/ iPads to be used in school and on educational visits | Pupils taught about sending and receiving inappropriate content |
| Communication via Games Consoles | * Accessing of unsuitable content. * Sending and receiving messages/photos with inappropriate content | Pupils  Teachers  Support staff | No games consoles permitted in school or on school visits | Pupils taught about sending and receiving inappropriate content |
| Communication via Wireless Technology Including Cyber-Bullying(See Section 6 above) | Sending and receiving messages with inappropriate content. | Pupils  Teachers  Support staff | In school all communication is via C2k Network | Pupils taught about sending and receiving inappropriate content outside school.  Pupils encouraged to report incidents of cyber-bullying to their parents/ guardians, the school and if appropriate, the PSNI.  School keeps record of Cyber-Bullying Incidents |
| Communication via online forums such as Fronter. | Sending or receiving inappropriate or offensive content. | Pupils  Staff | Monitoring of content exchanged | Pupils aware of acceptable use and guided to use forums for specific/ focused discussions. |
| Use of iPads for internet use and communication | * Accessing inappropriate or offensive content. * Attempts to communicate outside educational purposes. | Pupils  Staff | Filter in place other than that provided by c2k.  Use of ipads supervised and monitored. | Pupils aware of acceptable use and of the procedures for reporting breaches of this. |

Appendix 4.

**Online safety.**

**What to do if you are concerned about something you see/ hear online.**

I have a concern about something I have seen or heard online or about someone else’s online activity/ behaviour.

If I am still concerned, I can talk to the Designated Teacher/ Principal for Child Protection

If I am still concerned, I can talk/write to the

Chairperson of the Board of Governors

I can talk to the class teacher/ Classroom Assistant or other trusted adult

**At any time I can talk to:**

**Childline - 0800 1111**

**Social Services - (Single Point of Entry Team) 030 0123 4333**

**Or**

**PSNI at the Public Protection Unit Tel: 999 (Emergency) or 101 (Non-Urgent)**

**CEOP- Child Exploitation and Online Protection Centre**

[**www.ceop.police.uk**](http://www.ceop.police.uk)

**Appendix 5: Useful Contacts**

|  |  |  |
| --- | --- | --- |
| **Name** | **Address** | **Contact** |
| **C2k** |  | 09706011666 |
| **Northern Health & Social Care Trust- Single Point Entry (SPOE, Referral Gateway) Team** | Oriel House,  8 Castle Street,  Antrim  BT41 4JE | 030 0123 4333  Or  028 94442 4459 |
| **PSNI- Public Protection Unit**  **PSNI Schools Officer, Sue Wright** |  | [susan.wright@psni.pnn.police.uk](mailto:susan.wright@psni.pnn.police.uk)  02887750503 |
| EA Child Protection Support Service (CPSS) |  | 02895 985590 |

### Appendix 5: Acceptable Use

### An Acceptable Use of the Internet

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

* On the network, I will only use my own login username and password.
* I will keep my username and password private.
* I will not access other people’s files without their permission.
* I will not change or delete other people’s work/files.
* I will ask permission before entering any website, unless my teacher has already approved that site.
* I will use the Internet for research and school purposes only.
* I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.
* I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
* When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
* I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
* If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
* I will not bring in handheld devices, memory sticks or hard drives from home to use in school unless I have been given permission by my class teacher.
* I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
* I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.
* I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/cares will be informed.

**Churchill Primary School**

# Acceptable Use Agreement

# For Pupils

# Please complete and return this form to your child’s class teacher

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Pupil’s Name |  | | **Class Teacher** | |  | |
| As a school user of the Internet, I agree to follow the school rules on its’ use. I will use the network in a responsible way and observe all the restrictions explained to me by my school. | | | | | | |
| **Pupil Name (print)** | |  | |  | | |
| **Pupil Signature** | |  | | **Date** | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Parents Name |  | | | |
| As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email\*. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information. | | | | |
| **Parents Name (print)** | |  |  | |
| **Parents Signature** | |  | **Date** |  |

### \*P7 only

### Churchill Primary School Acceptable Use Agreement For Staff

The 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 Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

* All Internet activity should be appropriate to staff professional activity or the pupils’ education
* Access should only be made via the authorised account and password, which should not be made available to any other person
* Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
* Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
* Use for personal financial gain, gambling, political purposes or advertising is forbidden
* Copyright of materials must be respected
* Posting anonymous messages and forwarding chain letters is forbidden
* As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
* Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

Name: ………………………………………. Date:…………………………….

Signed:………………………………………………………..