E Safety and Acceptable Use Policy

September 2021

E-Safety and Acceptable Use Policy

September 2021

Policy Review

This policy will be reviewed in full by the Governing Body on an annual basis.

The policy was last reviewed and agreed by the Governing Body on _____

It is due for review in July 2022

Head Teacher:	**Date:**
Chair of Governors:	**Date:**

Contents:

Appendices

Rationale

This policy has been updated to reflect the GDPR and is a key document for all staff. It is covered in the induction of all new staff and volunteers. It is reviewed with staff annually.

As a school working with our local, national and international communities, ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

'ICT' covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. 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
- E-mail and Instant Messaging
- APPs
- Snapchat
- 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 with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Toner Avenue School, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and

critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) apply to all school equipment at any time and all other equipment brought onto the school premises by staff. Staff and visitors (including students) should seek the Head Teacher or Deputy's permission before bringing their own equipment onto the premises.

Staff must also adhere to their responsibilities to safeguard personal data at all times.

The policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices 1 and 2), does not stand-alone and needs to be seen as part of an holistic approach to keeping children and other members of the school community safe and protect their interests. The policy needs to be read in conjunction with other related policies and documents as listed below. Staff are made aware of these documents and how to access them.

School Policies and Documents	**Government and Local Authority Documents**
Safeguarding and Child Protection Policy Anti-Bullying Policy Behaviour Policy Dealing with Racist Incidents Policy	Working Together to Safeguard Children 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729914/

Health and Safety Policy Staff Handbook Home School Agreement Data Protection Policy Data Breach Policy Ipad Acceptable Use Agreement	Working_Together_to_Safeguard_Children-2018.pdf Inspecting E-Safety (January 2014) http://www.bettshow.com/files/inspecting_esafety_in_schools__david_brown.pdf Teaching Online Safety in Schools (June 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf Education for a Connected World Framework (2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf

The policy is reviewed on an annual basis although it will be updated as and when legislation changes.

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The school has appointed an E-Safety Co-coordinator (Acting Head, Mrs. Hutchinson). Any extra permission given by the Head or Deputy must be recorded **in writing** (e.g. memos, minutes from meetings) in order to be valid. The school also has appointed a Data Protection Officer – Bryan Chapman - who can be contacted at : bryan.chapman@chapmandis.co.uk

The E-Safety Co-coordinator and/or Head have the responsibility of ensuring this policy is upheld by all members of the school community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection,

the Prevent Duty – September 15), DPO and Local Authority Safeguarding Children Board.

INTERNET ACCESS

Why is Internet use important?

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up. Internet use is part of the statutory curriculum and is a necessary tool for learning. We have a duty to provide our students with quality Internet access as part of their overall learning experience.

Benefits to Education

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and galleries.
- Education and cultural exchange between pupils worldwide.
- Immediate access to up to the minute news and current events.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- The opportunity for staff to and pupils to discuss with experts in a variety of fields.
- Staff professional development through access to national developments, educational resources and good curriculum practice.
- Communication with support agencies, professional associations and colleagues
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administrative data with Local Authority other professional bodies.

Staff Internet Use

In accordance with GDPR, staff must only access computers using their own accounts. Staff use of the Internet is restricted to professional use only. The Internet on school computers should not be used for any political purposes, personal gain or social use e.g. personal E-mails, booking holidays, online

shopping, private financial matters or social networking. These restrictions also apply to any laptops that are taken off site for use at home.

- Staff must log off every time they leave the room.
- Passwords must not be saved to auto fill and must be kept secure.
- Staff use of USB memory sticks must be kept to an absolute minimum. Where a memory stick is used, staff must use encrypted memory sticks.
- No personal data is to be stored on the hard drives of any machines. Staff must save all personal data to the Google Drive account.
- Staff should regularly review the personal data they have saved electronically. Data should be deleted in line with the Retention Schedule. (See main office)
- YouTube items must not be 'live streamed' due to the potential for inappropriate content to appear.
- Images must be viewed and saved before using with children rather than live on-screen searches.
- Inappropriate use of the Internet will be subject to disciplinary action.

Keeping staff and pupils aware of their Conditions of Use

All staff and adults working in school will be given a copy of the 'Acceptable and Responsible Use of Internet Policy' and its importance explained. Users will be required to sign an agreement indicating their acceptance of school policy before being issued with a logon account. If they feel unprepared for Internet use then the Computing coordinator will spend time tutoring the basics to them. Reassurance and discussion are always available from the Computing coordinator.

Rules for Acceptable Use of IT will be posted near all computer systems (see Appendix 3).

Children will be refreshed at the beginning of every academic year of the rules of acceptable use of IT. These rules will also be referred to as appropriate through lessons.

Parental Support

Parents' attention will be drawn to the Acceptable and Responsible Internet Use document via the website and the school brochure. Internet issues will be handled sensitively to inform parents without undue alarm. A partnership approach with parents will be encouraged. Home use is increasing at possibly a faster rate than school use and parents must be made

aware/reminded of the dangers of unrestricted access. Supervised use of the Internet at home is encouraged. The school is available to discuss any issues/concerns about the Internet or other IT use. Parents will be given a copy of the school's 'Rules for Acceptable Use of IT' to refer to at home.

Parents will be offered advice and support around E-Safety through workshops provided on an annual basis.

Interested parents will be referred to organisations such as PIN (Parents Information Network), Parents Online and National Action for Children or advice sought from the Local Authority Advisor.

How will risks be managed and how will pupils learn how to evaluate Internet content?

As with a number of other social media sources, such as magazines, books and videos, the Internet contains material unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material by using South Tyneside's filtering system and children will not be allowed Internet access without the presence of a member of staff. Staff supervision is paramount in taking all reasonable precautions to ensure only appropriate material is accessed. Our aim is to provide a 'managed' risk rather than 'lock down' the internet to ensure children are prepared for use of the internet outside of school. The use of the Local Authority's filtering, together with the E-Safe software means that the risks are managed and children educated.

However, even with adult supervision, it is impossible to guarantee that particular types of material will never appear on a computer terminal of station. This is due to the international scale and linked nature of material on the Internet. The school cannot accept liability for inadvertent access to material accessed or to the consequences of such access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the matter must be brought immediately to the attention of the E-Safety Coordinator. The school will seek advice to determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the Children Safeguard Team or E-Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

The Prevent Duty (September 15) sets out school's responsibility to, "…ensure children are safe from terrorist and extremist material when accessing the internet in school". By using the Local Authority Filtering System, any

inappropriate material should not be able to be accessed in school. However, if a child does access any extremist material, either at home or at school, the E-Safety Coordinator must be informed immediately and the school's Safeguarding Procedure followed. (See Safeguarding and Child Protection Policy).

Methods to identify, assess and minimize risks will be reviewed annually. The Head Teacher (and E-Safety co-ordinator) will ensure that the Internet policy is implemented and compliance with the policy monitored.

Although the internet is an essential tool which has a positive impact on children's learning, we also have a responsibility to teach our children that information they receive may not always be accurate. Children will be supported to develop critical skills in selection and evaluation. Children will be expressly taught to question the reliability of sources and will learn to evaluate information that they find, including consideration of the origin, intent and accuracy of such information as appropriate to their age and stage of development. The tools used to search for information will be age-appropriate (for example, swiggle search engine will be used in KS2). Staff also need to be aware of the need for critical evaluation of information obtained by web-sites. Particular care should be taken when researching potentially emotive themes, such as the Holocaust.

How will filtering be managed?

It is the staff's responsibility to check the suitability of any websites they wish the children to use. Children must always be supervised when using the internet and should adhere to the Acceptable Use Policies which are in place. In addition, Internet Safety Rules are displayed in the computer suite and other locations where children have access to the internet (e.g. in classroom). Children are educated about the risks online as part of the Computing curriculum.

If staff or pupils discover unsuitable sites, the monitor must be switched off and the Head or Deputy alerted. The URL will be recorded and the incident recorded or the concern escalated as appropriate.

Children and staff are aware that the school receives weekly E-Reports and that any inappropriate key strokes / searches are immediately flagged up.

URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.

How will information systems security be maintained?

- Websites are filtered at source. There will be no changes without the Head Teacher's permission. All changes need to be recorded in writing.
- Virus protection software is installed and is updated as is reasonably practicable.
- Security strategies will be discussed with the Local Authority as appropriate.
- The use of CD-ROMS and memory USB sticks by children is forbidden. Staff's use of memory sticks should be kept to a minimum – work should be saved on their secure server area. Any USB sticks which are used to save data relating to children (including personal details such as names, assessment data etc.) must be encrypted and password protected. Staff should also be mindful of viruses when using memory sticks between machines.
- Laptops which contain sensitive data (as described above) must be encrypted and password protected.
- The Computing coordinator, with the help of the school technician, will ensure system capacity is reviewed to take the ever-increasing use of the Internet.
- Children's work is subject to monitoring at any time by that child's class teacher, the Computing coordinator, the E-Safety coordinator or the Head Teacher.
- Children must store any saved files within their allocated drive and folder.
- E-Safe will be used to monitor usage.
- Direct teaching of E-Safety during each half term as part of the Computing Scheme of Work.
- No staff are permitted to download or install any software without obtaining consent from the Head Teacher.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the GDPR 2018.

Staff are responsible for familiarity with the updated Data Protection Policy, which outline the GDPR.

When working from home, staff are responsible for ensuring that all data is only saved via the Google Drive and is not stored locally on hard drives or memory sticks.

Any personal data which is written down must be shredded when no longer needed and must not be left in public view. A clear desk policy should be adhered to by all staff.

Procedures for Reporting A Data Breach.

A 'data breach' can be confirmed or suspected. Either way it must be reported. A data breach is where data is (or potentially has been) compromised in terms of its confidentiality, integrity or availability of systems or data which could cause damage to Toner Avenue Primary School's information assets and / or reputation. Further details can be found in the Data Breach Policy (4.3)

All incidents will be reported to the Head Teacher immediately. In the absence of the Head, the Deputy will take responsibility for dealing with the incident. All incidents will be logged on the Data Breach Reporting Form (See appendix 1 of Data Breach Policy or via the website at: http://www.toneravenue.uk/gdpr-and-data-protection/

Procedures for Reporting Inappropriate use of I.T.

All incidents will be reported to the Head Teacher. In the absence of the Head, the Deputy will take responsibility for dealing with the incident. All incidents will be logged in the E-Safety Incident Log.

How will Internet access be authorised?

The school agrees to Internet access based on educational or professional development needs without prior permission.

Other reasonable use of the Internet may be allowed but must be agreed to by the School Management Team before use.

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 or pupil may leave or a pupil's access be withdrawn.

At Key Stage 1 Internet access will only be through adult or teacher demonstration. Children may access teacher prepared files or materials rather than open the Internet.

At Key Stage 2 Internet access will be granted to the whole class based on a lesson need that corresponds to the Computing or cross curricular Schemes of Work. Children must first have been given a suitable introduction to rules for responsible use of the Internet. They must also apply individually by agreeing to abide by the Acceptable and Responsible Internet Use Statement. (Appendix 2) Pupils will use an age-appropriate search engine (Swiggle) and online tools and online activities will be teacher-directed where necessary.

Pupils will be allowed supervised use of the Internet for research or reference outside of class time (e.g. break times or after school clubs).

Parents will be informed at the beginning of the academic year of supervised Internet access relevant to their education. Parents must sign and return a permission slip allowing this access (see Appendix 2).

How will E-mail be managed?

The use of E-mail within schools is an essential means of communication for both staff and pupils. Educationally, E-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an E-mail in relation to their age and good 'netiquette'.

The school gives all staff their own E-mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious E-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal E-mail addresses.
- E-mail sent to an external organisation should be written carefully and checked before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- All E-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about

themselves or others in E-mail communication, or arranging to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive E-mail. This information must be passed on to the E-Safety coordinator.
- Staff must inform the E-Safety coordinator if they receive an offensive E-mail.
- Staff should not use personal E-mail accounts during school hours or for professional purposes.
- Data should not be sent via email, when discussing individual children initials should be used and only between google school accounts.
- Any data that is required by 3rd parties EP, Child protection, transferring children etc, must be sent securely using egress or CTF transfers.
- Any correspondence with parents (for example, in the event of a lockdown) must be done through the Year Group email.

How will staff's E-Safety skills be developed?

- Our staff receive regular information and training on E-Safety issues in the form of full staff meetings and memos, including training from the Local Authority. This is done at least annually and as part of the Safeguarding update.
- New staff receive information on the school's acceptable use policy as part of their induction through their staff handbooks.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community. (See above).
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.
- The E-Safety policy is reviewed and shared with staff on an annual basis.

How will published content be managed?

- Parents will be asked to give their consent to allow their child's photographs to be published on the school website. This consent will be renewed on an annual basis.
- Staff must ensure they only put photographs of children with consent in the website file.
- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

How will social networking, social media and personal publishing be managed?

Social networking is now widely used to allow people to connect with people from around the world. At Toner Avenue, we encourage our children to think carefully before uploading personal information, the dangers associated with this and the difficulties of removing information once it has been published through our Computing curriculum as well as events such as ' E-Safety Day' and 'Safer Internet Day'. We aim to educate parents and carers about the dangers associated with Social Networking through parental surveys (annually) and invitations to workshops held by the Local Authority.

Staff are made aware (through the Acceptable Use Agreement) of the potential risks of using social networking sites. Staff who choose to us such sites must not accept friend requests from pupils (including former pupils) or parents and should ensure that any information they publish is in line with the expectations of their professional status.

By default the school will block access to social media and social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them and/or their location.

Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will e–Safety complaints be handled?

Complaints about Internet misuse will be dealt with under the School's complaints procedure.

Any complaint about staff misuse will be referred to the head teacher.

All E–Safety complaints and incidents will be recorded by the school, including any actions taken.

Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone," DCSF 2007

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents

- gives Head Teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted upon in line with the behaviour policy.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

All incidents of cyberbullying reported to the school will be recorded. All allegations will be investigated by a member of the Senior Leadership Team and any findings or actions recorded.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

OTHER COMMUNICATION TECHNOLOGIES.

Pupils Use of Personal Devices

Students are not allowed to have mobile phones with them in school. It is forbidden to send abusive or otherwise inappropriate text messages using facilities provided by the school network. School staff may confiscate a phone or device and ask the parent to collect it from the office. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence, the phone will be handed over to the police for further investigation.

Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Staff Use of Personal Devices

Staff are not recommended to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Where there is no alternative, staff must ensure that they withhold their number.

Any staff that access their work emails on a personal device, should be aware of the following:

- Follow guidelines highlighted earlier.
- Use only when necessary
- Ensure mobile phones are password protected when locked.
- Sign out of the email account when not in use.
- If using a mobile phone, ensure that all data is wiped before the device is sold or passed on.

- If the device is lost or stolen, data breach procedures should be followed.

Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances. Phones should not be out in class during lesson times.

If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

All photographs taken by staff of the children must be on school cameras. No personal camera or mobile phones should ever be used to take photographs of the children. All photographs should be downloaded to the 'staff shared' part of the server within twenty- four hours. Photographs stored will be reviewed on a regular basis and when they are no longer required. Staff are responsible for ensuring any parents who accompany visits do not take photographs on their own personal devices.

Photographs must not be stored on memory sticks or staff's private folder on the server.

Appendix 1

Toner Avenue Primary School

Acceptable Internet Use Statement: 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 pupils, 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 requesting Internet access should ensure they have read and understood the E-Safety Policy and should sign a copy of this Acceptable Use Statement and return it to the Head Teacher for approval.

- 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 system 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 an E-mail being received.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials must be respected.
- All Internet activity should be appropriate for staff professional activity or pupils' education.
- The same professional levels of language and content should be applied as for letters or other media, particularly as E-mail is often forwarded or may be sent inadvertently to the wrong person.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Users must only access those sites and materials relevant to their work in school.

- Users will be aware when they are accessing inappropriate material and should expect to have their permission to use the system removed.
- Staff should not give their password or E-mail address to pupils.
- Use of ICT and information systems will always be compatible with the professional role held by staff, whether using school or personal systems. This includes the use of E-mail, text, social media, social networking, gaming, web publications and any other devices or websites.
- Use of ICT will not interfere with work duties and will be in accordance with the school AUP and the Law.
- If staff bypass proxy /LAN settings then they are individually responsible for their actions and resulting outcomes.

I confirm that I have read and understand the E-Safety Policy and, by signing this Acceptable Use Statement, agree to the conditions detailed within.

Dear Parents,

As part of pupils' curriculum enhancement and the development of ICT skills, Toner Avenue School provides supervised access to the Internet.

In using this facility pupils may exchange electronic mail with recipients arranged by the school or be involved in researching information using suitable websites as part of their learning.

With Internet access comes the responsibility of the user to only access materials considered to be of educational value or in the context of a primary school. South Tyneside Local Authority and Toner Avenue's staff will make every effort to preserve free and safe Internet access to responsible pupils; however it is impossible to guarantee control of all accessed materials.

Users, must, therefore, be held responsible for the way they use ICT facilities at Toner.

I enclose a copy of rules for the acceptable use of IT here at Toner. It is recommended that if Internet access is allowed at home you adopt a similar set of rules and use an appropriate piece of security software.

Please return the permission slip below to your child's class teacher no later than **Friday**

Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours faithfully,

(Head Teacher)

_____

Permission for Internet Access

Parents/Carer's permission
I give permission for my child _____to access the Internet, following the terms set out in the *Rules for Acceptable Use of ICT* (attached).

Signed:_____Date:_____
Pupil's Agreement
or Responsible Internet Use.

Signed:_____Date:_____

Appendix 3

Rules for Acceptable Use of ICT

At Toner Avenue, we care about our pupils and want to promote mature users of IT. Many of our computers have Internet access. This is to help with our learning. The following rules are to keep you safe. Following them also helps us to use IT fairly and sensibly.

- I will only access the computer network with the allocated login name

- I will not open or access anyone else's file in any way.

- I will only use the school computers for schoolwork and homework.

- I will not bring in CD-ROMs or memory sticks from outside school and try to use them on school computers.

- I will ask permission from a member of staff before sending any work to any printer.

- I will only use ICT equipment with adult permission.

- I will only use the Internet with adult supervision.

- I will only E-mail people if my teacher has given me both permission and E-mail addresses to use and to send to.

- Any messages I write or send will be polite and responsible. (This includes messages sent to other pupils on Social Networks)

- I will not give out my personal details (home address or telephone number) or arrange to meet anyone over the Internet.

- To help protect other pupils and myself, I will tell a teacher if I see anything unpleasant or anything I am unhappy with when I am using a computer.

- If I receive anything unpleasant or messages I do not like I will tell my teacher immediately.

- I will only download or copy any file or image under the supervision of my teacher.

• I understand that the school may check my computer files and Internet sites I visit.