**Appletree Gardens First School**

**E Safety Policy 2018**

MCj03914060000[1]

Responsibility for the development and management of the policy

The development of this policy has been managed by the ICT Coordinator in conjunction with the Head Teacher, and through consultation with Staff, Pupils and the Local Education Authority.

It has been agreed by the School Teaching Staff

Senior Management Team

Governors

PTA

To be reviewed January 2019

* 1. **Who will write and review the policy?**

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, bullying and for child protection.

**●** The school has appointed an e–Safety Coordinator.

**●** The e–Safety Policy and its implementation will be reviewed annually.

**●** Our e–Safety Policy has been written by the school, building on the Kent e–Safety Policy, North Tyneside and government guidance.

**●** Our School Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders such as the PTA.

**●** The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

The School e-Safety Coordinator is … ……….............................................………………………………

Policy approved by Head Teacher: Jillian Burrell Date: ……………........

Policy approved by Governing Body: ……………..........................……………….. (Chair of Governors)

Date: …………..................…

The date for the next policy review is…......................……………

* 1. **Teaching and learning**

* + 1. **Why is Internet use important?**

**●** The Internet is an essential element in 21st century life for education, business and social interaction.

**●** The school has a duty to provide students with quality Internet access as part of their learning experience.

**●** Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

**●** The purpose of Internet use in Appletree Gardens First School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management information and business administration systems.

* + 1. **How does Internet use benefit education?**

Benefits of using the Internet in education include:

**●** access to worldwide educational resources including museums and art galleries;

**●** educational and cultural exchanges between pupils worldwide;

**●** access to experts in many fields for pupils and staff;

**●** collaboration across networks of schools, support services and professional associations;

**●** access to learning wherever and whenever convenient.

* + 1. **How can Internet use enhance learning?**

**●** The school’s Internet access will be designed to enhance and extend education.

**●** Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

**●** The schools will try to ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

**●** Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

**●** Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils’ age and ability.

**●** Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

**●** Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

* + 1. **How will pupils learn how to evaluate Internet content?**

**●** Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**●** Pupils should use age-appropriate tools to research Internet content.

**●** The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

**Managing Information Systems**

* + 1. **How will information systems security be maintained?**

**●** The security of the school information systems and users will be reviewed regularly.

**●** Virus protection will be updated automatically.

**●** Portable media may not used without specific permission followed by an anti-virus /malware scan.

**●** Files held on the school’s network will be regularly checked.

**●** The Computing coordinator and Computing Technician will review system capacity regularly.

**●** The use of user logins and passwords to access the school network will be enforced.

* + 1. **How will email be managed?**

**●** Pupils may only use approved email accounts on the school system (ntlp).

**●** Pupils must immediately tell a designated member of staff if they receive offensive email.

**●** Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

**●** 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.

* + 1. **How will published content be managed?**

**●** The contact details on the website and learning platform should be the school address, email and telephone number. Staff or pupils’ personal information must not be published.

**●** The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

**●** The school website will comply with the school’s guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

* + 1. **Can pupils’ images or work be published?**

● 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 or Twitter, particularly in association with photographs.

● Written permission from parents or carers will be obtained before images/videos of pupils are electronically published (This is part of the school’s admission paperwork)

● Pupils work can only be published with their permission or the parents.

● Written consent will be kept by the school where pupils’ images are used for publicity purposes, until the image is no longer in use.

* + 1. **How will social networking, social media and personal publishing be managed?**

**●** North Tyneside will control 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. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

**●** 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.

* + 1. **How will filtering be managed?**

**●** The school’s broadband access will include filtering appropriate to the age and maturity of pupils.

**●** The school will work with the LA and to ensure that filtering policy is continually reviewed.

**●** The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.

**●** If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

**●** The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

**●** Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Police or CEOP

* + 1. **How are emerging technologies managed?**

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

● Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

* + 1. **How should personal data be protected?**

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

* 1. **Policy Decisions**
     1. **How will Internet access be authorised?**

● The school will maintain a current record of all staff and pupils who are granted access to the school’s electronic communications.

● All staff will read and sign the ‘Acceptable ICT Use Agreement’ before using any school Computing resources.

● Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

● All visitors to the school site who require access to the schools network or internet access will be asked to read and sign the Acceptable Use Policy.

● Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

● When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

● At Key Stage 1 pupils’ access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.

● At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

**1.4.2 How will risks be assessed?**

**●** The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor North Tyneside can accept liability for the material accessed, or any consequences resulting from Internet use.

**●** The school will audit Computing use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

**●** Methods to identify, assess and minimise risks will be reviewed regularly.

* + 1. **How will the school respond to any incidents of concern?**

● All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).

● The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.

● The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

● The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.

● The school will inform parents/carers of any incidents of concerns as and when required.

● After any investigations are completed, the school will debrief, indentify lessons learnt and implement any changes required.

● Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children’s Safeguard Team or e-Safety officer and escalate the concern to the Police

● If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children’s Officer or the County e-Safety Officer.

● If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other school in North Tyneside.

* + 1. **How will e–Safety complaints be handled?**

**●** Complaints about Internet misuse will be dealt with by a senior member of staff.

**●** 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.

**●** Pupils and parents will be informed of the complaints procedure.

**●** Parents and pupils will need to work in partnership with the school to resolve issues.

**●** All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

**●** Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children’s Safeguard Team to establish procedures for handling potentially illegal issues.

**●** 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.

* + 1. **How is the Internet used across the community?**

● The school will liaise with local organisations to establish a common approach to e–Safety.

● The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

● The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

● The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

* + 1. **How will Cyberbullying be managed?**

**●** 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 antibullying and behaviour.

**●** All incidents of cyberbullying reported to the school will be recorded.

**●** Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

**●** The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

**●** Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school’s e-Safety ethos.

**●** 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.
  + 1. **How will Learning Platforms be managed?**

**●** Computing Coordinator, SLT and staff will regularly monitor the usage of the NTLP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.

**●** Pupils/staff will be advised about acceptable conduct and use when using the NTLP.

**●** Only members of the current pupil, parent/carers and staff community will have access to the NTLP.

**●** All users will be mindful of copyright issues and will only upload appropriate content onto the NTLP.

**●** When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

**●** Any concerns about content on the NTLP may be recorded and dealt with in the following ways:

1. The user will be asked to remove any material deemed to be inappropriate or offensive.
2. The material will be removed by the site administrator if the user does not comply.
3. Access to the NTLP for the user may be suspended.
4. The user will need to discuss the issues with a member of SLT before reinstatement.
5. A pupil’s parent/carer may be informed.

**●** Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

* + 1. **How will mobile phones and personal devices be managed?**

**●** The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use Policy.

**●** The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

**●** School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. 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.

**●** Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times and pupil’s phones should be handed in to the school office.

**●** The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

**●** 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.

**Pupils Use of Personal Devices**

**●** If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

**●** Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

**Staff Use of Personal Devices**

● Staff are not permitted 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.

● 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 times unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

● Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

● If a member of staff breaches the school policy then disciplinary action may be taken.

* 1. **Communication Policy**
     1. **How will the policy be introduced to pupils?**

● All users will be informed that network and Internet use will be monitored.

● An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.

● Pupil instruction regarding responsible and safe use will precede Internet access.

● An e–Safety module will be included in the PSHE, Citizenship and/or Computing programmes covering both safe school and home use.

● e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.

● e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.

● Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

● Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

* + 1. **How will the policy be discussed with staff?**

**●** The e–Safety Policy will be formally provided to and discussed with all members of staff.

**●** To protect all staff and pupils, the school will implement Acceptable Use Policies.

**●** Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

**●** The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

**●** All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

* + 1. **How will parents’ support be enlisted?**

**●** Parents’ attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.

**●** A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.

**●** Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.

**●** Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it’s implications with their children.

**●** Information and guidance for parents on e–Safety will be made available to parents in a variety of formats if required.

**●** Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

**Schools e-Safety Audit**

This self-audit should be completed by the member of the Senior Leadership Team (SLT)

responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

|  |  |  |
| --- | --- | --- |
| The school has an e-Safety Policy that complies with CFE guidance. | | **Y/N** |
| Date of latest update: | | |
| Date of future review: | | |
| The Policy was agreed by governors on: | | |
| The Policy is available for staff at | | |
| And for parents and carers at | | |
| The responsible member of the SLT is: | | |
| The governor responsible for e-safety is: | | |
| The Designated Child Protection Coordinator is : | | |
| The e-Safety Coordinator is : | | |
| Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy? | **Y/N** | |
| Has up-to-date e-safety training been provided for all members of staff? (not just teaching Staff) | **Y/N** | |
| Do all members of staff sign an Acceptable Use Policy on appointment? | **Y/N** | |
| Are all staff made aware of the schools expectation around safe and professional online behaviour? | **Y/N** | |
| Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern? | **Y/N** | |
| Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained? | **Y/N** | |
| Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)? | **Y/N** | |
| Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? | **Y/N** | |
| Do parents/carers or pupils sign an Acceptable Use Policy? | **Y/N** | |
| Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced? | **Y/N** | |
| Has a Computing security audit been initiated by SLT? | **Y/N** | |
| Is personal data collected, stored and used according to the principles of the Data Protection Act? | **Y/N** | |
| Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)? | **Y/N** | |
| Has the school filtering been designed to reflect educational objectives and been approved by SLT? | **Y/N** | |
| Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT? | **Y/N** | |
| Does the school log and record all e-Safety incidents, including any action taken | **Y/N** | |
| Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis? | **Y/N** | |

**e-Safety Contacts and References**

**CEOP** (Child Exploitation and Online Protection Centre): [www.ceop.police.uk](http://www.ceop.police.uk)

**North Tyneside e-Safety Team:** Tel: 0191 643 2525

**Childline:** [www.childline.org.uk](http://www.childline.org.uk)

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

**Child Protection in Education:** Lisa Wardingham – LSCB (Local Safeguarding

Children’s Board) Training and Development Officer for Schools –

lisa.wardingham@ntlp.org.uk – 0191 643 8079

**Click Clever Click Safe Campaign:** <http://clickcleverclicksafe.direct.gov.uk>

**Cybermentors:** [www.cybermentors.org.uk](http://www.cybermentors.org.uk)

**Digizen:** [www.digizen.org.uk](http://www.digizen.org.uk)

**Internet Watch Foundation** (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)

**North Tyneside E-Safety Guidance:** [www.ntlp.org.uk/external/?sid=3289](http://www.ntlp.org.uk/external/?sid=3289)

**Northumbria Police:** In an emergency (a life is in danger or a crime in progress) dial

999. For other non-urgent enquiries contact Northumbria Police via 101. Also visit

[www.northumbria.police.uk](http://www.northumbria.police.uk)

**North Tyneside Local Safeguarding Children Board:**

[www.northumbria.gov.uk/browse.shtml?p\_subjectCategory=486](http://www.northumbria.gov.uk/browse.shtml?p_subjectCategory=486)

**Kidsmart**: [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

**Teach Today:** <http://en.teachtoday.eu>

**Think U Know website**: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**Virtual Global Taskforce** — Report Abuse: [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com)

Foundation Stage and Key Stage 1

|  |  |  |
| --- | --- | --- |
| **Think then Click** | | |
| These rules help us to stay safe on the Internet | | |
| We only use the internet when an adult is with us. | We only use the internet when an adult is with us |  |
|  | We can click on the buttons or links when we know what they do. | We only use the internet when an adult is with us. |
| We only use the internet when an adult is with us. | We can search the Internet with an adult. |  |
|  | We always ask if we get lost on the Internet. | We only use the internet when an adult is with us. |
| We only use the internet when an adult is with us. | We can send and open emails together. |  |
|  | We can write polite and friendly emails to people that we know. | We only use the internet when an adult is with us. |

Key Stage 2

|  |
| --- |
| **Think then Click** |
| e-Safety Rules for Key Stage 2 |
| * We ask permission before using the Internet. * We only use websites that an adult has chosen. * We tell an adult if we see anything we are uncomfortable with. * We immediately close any webpage we not sure about. * We only e-mail people an adult has approved. * We send e-mails that are polite and friendly. * We never give out personal information or passwords. * We never arrange to meet anyone we don’t know. * We do not open e-mails sent by anyone we don’t know. * We do not use Internet chat rooms. |

**E-SAFETY INCIDENT REPORTING FORM**

|  |  |
| --- | --- |
| Date of incident: |  |
| Member of staff reporting incident: |  |
| Url, (web address) of incident: |  |
| Copy of screens/evidence saved to: |  |
| Location of incident (room): |  |
| Computer number if known: |  |
| Details: |  |
| Passed to: | Mr D Jenson  Miss C Stamp  Mrs Wilkinson  Mrs Burrell |
| Action taken |  |