# Purston Infant School
# E-Safety Policy & ICT Acceptable Usage Agreement (AUA)

## Rationale

As a Community 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.

Information and Communications Technology 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
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- i-pads
- 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 Purston Infant School, we understand the responsibility to educate our children 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.

Both this policy and the Acceptable Use Agreements (for all staff, governors and visitors) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, digital video equipment, etc) and technologies owned by children and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

## 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. This responsibility is delegated to the Head. Any extra permission given by the Head must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The named person (Safeguarding Officer Miss Leather) has 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, Becta, CEOP (Child Exploitation and Online Protection), Childnet and Local Authority Safeguarding Children Board.

This policy, supported by the school's acceptable use agreements for staff, governors and visitors (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, safeguarding policy and behaviour/pupil discipline (including the anti-bullying) policy.

**E-safety skills development for staff**

- Our staff receive regular information and training on e-safety issues in the form of full staff meetings and memos.
- New staff receive information on the school's acceptable use policy as part of their induction.
- 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.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

**Communicating the school e-safety messages**

- E-safety rules will be posted in all networked rooms and discussed with the children at the start of each year.
- Children will be informed that network and Internet use will be monitored.
- E-safety posters will be prominently displayed, especially in the ICT suite.

**E-Safety in the Curriculum**

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the children on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. We regularly monitor and assess our children's understanding of e-safety.

- The school provides opportunities within a range of curriculum areas and discrete ICT lessons to teach about e-safety (in accordance with the medium term planning.)
- Educating children on the dangers of technologies that maybe encountered outside school may also be done informally when opportunities arise.
- Children are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Children are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Children are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Children are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/CEOP report abuse button.
- Children are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

**Password Security**

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have access to this through Administrator Rights on the network. The children from UFS upwards have individual logins and storage folders on the server. Staff and children are regularly reminded of the need for password security. Staff have encrypted USB sticks.

**Data Security**

The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher. Data can only be accessed and used on school computers or laptops, unless otherwise authorised by the Headteacher, having consideration for internet security. Staff are aware they must not use their personal devices for accessing any school/pupil data, unless authorised by the Headteacher. Any sensitive information regarding children, is password protected when forwarding on to other agencies via e-mail. Only approved encrypted USB memory sticks will be used to store data.

**Managing the Internet**

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.

- All staff must read and agree to the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with children.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

**Infrastructure**

- School internet access is controlled through web filtering software.
- Staff and children are aware that school based email and internet activity can be monitored and explored further if required.
- In the rare event that staff or children discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the headteacher.
- It is the responsibility of the school, by delegation to the technical support; to ensure that Anti-virus protection (Sophos) is installed and kept up-to-date on all school machines.
- Children and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.
- If there are any issues related to viruses or anti-virus software, the admin staff should be informed through the 'Computer Problems' book held in the school office.

**Managing other Web 2 technologies**

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our children to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to unmonitored social networking sites such as Facebook to children within school.
- There should be no communication between staff and children, staff and parents, through social networking sites such as Facebook.
- All children are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Children are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Children are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our children are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Children are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our children are asked to report any incidents of cyber bullying to the school.

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with children using the LA Learning Platform or other systems approved by the Head Teacher.

**Mobile technologies**
Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

**Personal Mobile devices (including phones)**

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device, unless deemed an emergency. The first point of contact is always the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

**Managing e-mail**
The use of email within most schools is an essential means of communication for both staff and children. 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 children need to understand how to style an email in relation to their age and good 'netiquette'
The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails 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 children, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Children may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All children use a class/ group email address.
- 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.
- Children must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the Headteacher if they receive an offensive e-mail.

**Safe Use of Images**

## Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of children) and staff, the school permits the appropriate taking of images by staff and children with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of children, this includes when on school trips, unless authorised by the Headteacher. Any images recorded should be deleted from the equipment once downloaded to the school network.
- Children are permitted to use personal digital equipment such as cameras on school trips, only with the consent of the class teacher. With the consent of the class teacher, children are permitted to take digital cameras from school to record images and can download these images on the school network.

## Publishing pupil’s images and work

On a child’s entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school’s Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school’s communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. If the school is not notified permission will be assumed.
Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Children’s full names will not be published alongside their image and vice versa. E-mail and postal addresses of children will not be published.
Before posting children’s work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

## Storage of Images

Images/ films of children are stored on the school’s network.

- Children and staff are not permitted to use personal portable media for storage of images (e.g., Approved encrypted USB sticks) without the express permission of the Head Teacher
- Rights of access to this material are restricted to the teaching staff and children within the confines of the school network/ Learning Platform.
- Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

## Misuse and Infringements

### Complaints

- Complaints relating to e-safety should be made to the Head Teacher and followed up in accordance with the complaints procedure.

### Inappropriate material (see ICT Acceptable Use Agreement)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head Teacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Admin staff, depending on the seriousness of the offence; investigation by the Head Teacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences. In the event that this is the Head Teacher, this would be carried out by the Chair of Governors.
- Users are made aware of sanctions relating to the misuse or misconduct.

## Equal Opportunities

### Children with additional needs

The school endeavours to create a consistent message with parents for all children and this in turn should aid establishment and future development of the schools' e-safety rules. However, staff are aware that some children may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

### Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
    - Information sessions
    - Posters
    - Learning Platform postings/links to further information
    - Newsletter items
- Parents will be advised that the use of social network spaces (eg Facebook) outside school is inappropriate for primary aged children.
- Parents/carers are expected to reinforce the guidance from school when using technologies at home. The school will not be responsible for communications between children outside school through social networking sites.
- Parents are asked to sign to say they will not use any images (photos or video) from school performances, assemblies, sports days etc on social media sites in accordance with confidentiality and data protection.