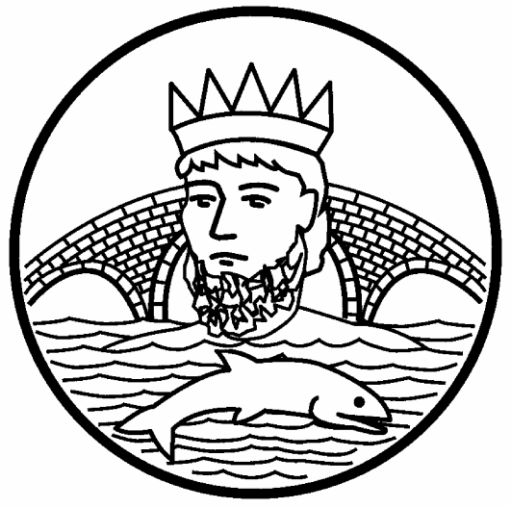
King Athelstan Primary School



E-Safety Policy

King Athelstan Primary School – Inspiring Excellence

We believe in the relentless pursuit of excellence to achieve high standards.

We are driven to inspire our school community to be aspirational, ambitious and to "dream big."

We empower children with choices which prepare them for a life of opportunity.

We teach children that hard work delivers success; we encourage children to take risks and ask brilliant questions in order to inspire a love and passion for learning.

We teach children to think.

We put children's happiness and welfare at the heart of everything we do.

We value friendship, kindness and respect.

We celebrate the excellence in each individual.

We expect families to work with us to form a strong team around every child.

We teach children to be good citizens.

We are proud of our school: Come as you are and leave us great.

Responsibility: Computing Coordinator (Tom Channing)

Date reviewed: March 2018 **Next review date: September 2020**

1. Overview

Our e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the Senior Leadership Team and approved by Governors. It will be reviewed annually.

It is our duty to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings. This Policy document is drawn up to protect all parties – the children, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Creating a safe Computing learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents/carers.

Roles and Responsibilities

Our school e-Safety Co-ordinator is the Computing lead. Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinator ensures the Headteacher, Senior Leadership Team and Governors are updated as necessary.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff are reminded / updated about e-Safety matters at least once a year and always during staff induction at the beginning of each academic year.

E-safety is included in the curriculum and we ensure that every pupil has been educated about safe and responsible use. Pupils are taught how to control and minimise online risks and how to report a problem. This is taught at the beginning of a computing topic where appropriate e.g. email or using search engines and is also taught where appropriate through the PSHE curriculum during the topics 'Getting on and Falling Out' and 'Anti-Bullying'.

Parents/carers sign and return an e-safety/Acceptable Use Policy form when their child joins the school as part of the Home School Agreement. Children are reminded of this at the beginning of each academic year by their class teacher as part of their first Computing lesson.

2. Managing the Internet Safely

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All children are taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. In line with school policies that protect children from other dangers, they are provided with as safe an Internet environment as possible.

The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

The use of school equipment to view or transmit inappropriate material is "unauthorised" and infringements will be dealt with. All reasonable and appropriate steps have been taken to protect children. These include technical and policy actions and an education programme for pupils and staff. Training/workshops will be offered to parents/carers to support e-safety at home.

Internet filtering is a key service. We have up-to-date anti-virus, anti-spyware and anti-spamware software and approved firewall solutions installed on the network.

To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into users' files through Internet use, staff and children are not able to download executable files and software. Unfortunately, inappropriate materials will inevitably get through any filtering system. So, we are vigilant and alert so that sites can be blocked.

Filtering is now the responsibility of the school. Process for unblocking websites – teachers ask Computing coordinator, consultation with HT or DHT, unblock site accordingly.

3. Managing e-mail

Where the school receives nuisance or bullying e-mails and the e-mail address of the sender is not obvious, it is possible to track the address using 'e-mail' tracking software. In this situation other school policies such as the behaviour or anti-bullying policy would be followed.

In the school context, e-mail should not be considered private and we reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of children and the preservation of human rights, both of which are covered by recent legislation.

Children are made aware of the risks and issues associated with communicating through e-mail and are taught strategies to deal with inappropriate e-mails. This is part of the school's e-Safety education programme.

4.Use of digital and video images

The school website and Twitter feed are an important, public-facing communication channel. The Leadership Team oversees / authorises the website's content and checks suitability. Only designated members of staff have the authority to upload content into sections of the website. In most cases this will be the Senior Leadership Team, the Business Manager or the Computing Coordinator.

For information on the use of children's images and work on the website please refer to the Pupil Image Release policy. Links to any external websites will be thoroughly checked before inclusion on the school website to ensure that the content is appropriate both to the school and for the intended audience. Staff and children will report any inappropriate use of images to the e-Safety Coordinator.

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Children are taught about how images can be abused in their e-Safety education programme;

5. Social media and e-safety out of school

The school is aware that many children have wide access to the internet and social media. Whilst it is the parents/carers role to monitor and manage this, the school will provide relevant advice and information to support them. School will encourage parents to monitor their children's social media and report concerns to the police. School may become involved if social media incidents affect the wellbeing of children in school. The school may report concerns to the SPA (Single Point of Access) in line with the Safeguarding Policy.

6. Managing Equipment

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

To ensure the network is used safely this school:

- Provides children with an individual network log-in username and password from Year 1.
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that children should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for children and one for staff. Staff and children are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Requests that staff and children switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
- Maintains equipment to ensure Health and Safety is followed;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Does not allow any outside Agencies to access our network remotely except AzteQ who manage the IT system
- Uses the secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

7. How will infringements be handled?

Whenever a child or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Senior Leadership Team in line with the school behaviour policy for children or with advice from the local authority for staff. The child protection policy will also be referred to if appropriate.

If inappropriate web material is accessed:

1. Appropriate technical support will filter the site
2. The LA and/or IT will be informed

Serious infringements by children

Contact will be made with parents/carers, the local authority and the police as appropriate. Examples of these infringements are;

- Continued sending of emails or instant messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, violent or pornographic
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Infringements by staff

Advice will be sought from the appropriate Local Authority department if a member of staff infringes on this policy. The police or other agencies will be contacted as appropriate.

In the case of safeguarding concerns being apparent, the member of staff will be **immediately suspended** and the Police will be called: see the free phone number **0808 100 00 40**.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reporting_abuse.html
http://www.iwf.org.uk

Rules for Responsible Internet Use for children

The school has computers with internet access to help our learning. These rules will help keep us safe and help us be fair to others.

Using the computers:

- I will only access the computer system with the login and password I have been given;
- I will not access other people's files;
- I will not bring in disks or CDs from outside school and try to use them on the school computers.

Using the internet:

- I will ask permission from a teacher before using the internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the way I use the computer including internet sites I visit;
- I will not complete and send forms or sign up to sites without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.

Using e-mail:

- I will ask permission from a teacher before checking my e-mail;
- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;
- I understand that e-mail messages I receive or send may be read by others;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or my teacher has approved;
- I will only send an e-mail when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number;
- I will not use e-mail to arrange to meet someone outside school hours.

Signed …….. Pupil (parents/carers to sign for Nursery & Reception pupils)

REVIEW OF POLICY

Signed on behalf of the Governors: _____

Date: _____