ALDERMAN JACOBS PRIMARY SCHOOL (ACADEMY TRUST)

E-Safety Policy

Aim

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology

- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

Roles & Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
  - Chair the e-Safety Committee

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate Continued Professional Development (CPD) in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.
- All incidents of sexting are dealt with through the Safeguarding and Child Protection policy and procedures.

E-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to *Jenny Smith*

(*Note: this is often a combined role, e.g. Child Protection Officer, ICT Coordinator*)

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Liaise with Child Protection Designated Personnel on incidents of internet safety issues
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  o Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  o Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
  o Any e-safety technical solutions such as Internet filtering are operating correctly.
  o Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
  o Passwords are applied correctly to all users regardless of age. Passwords for staff will be subject to change every 3 months.
  o Pupil passwords, as children only use the network under supervision do not need changing, as advised by County support.
  o The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.

- Any e-safety incident is treated as a Child Protection matter and appropriate measures taken. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters, information on the school website and an annual parent's e-safety event, the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Achievement Committee

Chaired by the Governor responsible for e-Safety, the achievement Committee is responsible:

- To advise on changes to the e-safety policy.
- To establish the effectiveness (or not) of e-safety training and awareness in the school.
- To recommend further initiatives for e-safety training and awareness at the school.

Established from volunteer students, parents, e-Safety Officer, responsible Governor and others as required the achievement Committee will meet on a termly basis.

Definitions

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents and other relatives.

Safeguarding is a serious matter; at AJS we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the AJS website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Code of Conduct Policy. A copy of this policy and the Students Acceptable Use Code of Conduct Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Technology

AJS uses a range of devices including PC's, laptops, iPads, Kindle Fire.   In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

We use Lightspeed software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is

determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering

We use county email software that prevents any infected email to be sent from the school or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption

All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff and students will be unable to access any device on the network without a unique username and password. Staff passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Devises that are not password enabled such as an iPad should be cleared of all personal data and files after use.

Anti-Virus

All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives (if you allow them) are to be scanned for viruses before use.

Safe Use

Internet

Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Google Suite for Education

Students are permitted to use Google Suite for Education and will be issued with their own school based Google account. Each class has an online 'Classroom' which every pupil can access using any internet enabled device. All school online activity should be done through this system and monitored in the first place by the class teacher. Staff should be proactive in teaching the children to be responsible online citizens and encouraging positive online activity and reactive to deal appropriately with any misuse. Child protection procedures should be followed where necessary.

Parents are encouraged to work with their children within the Google Classroom, but do not have permission to use any of the data held within (see Acceptable Use Policy for further guidance)

Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

At present pupils do not have access to the email feature although this could be activated should it be required.

Photos and videos

Digital media such as photos and videos are covered in the schools' Mobile Phone and Camera Use Policy, and is re-iterated here for clarity. All parents have an option to refuse permission for their child to be photographed or videoed at the beginning of each academic year.

Social Networking

There are many social networking services available; AJS is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within AJS and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school within Google Suite
- Facebook – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be monitored by the class teacher or page host.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Instant Chat and Message Apps

The minimum age to use these apps is 13 years old. If school becomes aware of use of these apps by pupils, who are under the minimum age, then the parents/carers will be contacted by the Child Protection Officer.

Pupils, especially those in the older year groups choose to communicate with each other and with online 'friends' using instant messaging and chat apps like Instagram and WhatsApp? Although there are no plans to use these tools in school, teachers should be aware of their use and be prepared to deal with any potential issues as they arise. Adults in school should not underestimate the power of these apps and the potential influence that they have on the lives of the young people in school. Open and frank discussions about online responsibility should take place throughout the school year not just in designated e-safety sessions.

Live Streaming

The increased popularity of 'Live Streaming' is an area that all staff should be mindful of, due to the potential of abuse. Although this activity should not be taking place in school it is still an area where staff will need to be vigilant. All staff should be prepared to discuss this in a neutral way through internet safety sessions.

Notice and take down policy

Should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents

Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out a child protection form.

Any issues concerning the production and distribution of sexting images involving anyone under the age of 18 is illegal and needs careful management for all those involved. If a device is involved it will be confiscated and set to flight mode, where possible, or switched off while investigations are carried out.

Radicalisation and Extremism

All staff are aware through the annual staff PREVENT training of their roles and responsibilities in reducing the potential for groups or individuals of becoming involved in potentially extreme groups. Any suspicions must be dealt with immediately using the school child protection policy and referred to the police as appropriate.

Tapestry Online Learning Journal

Policy Statement ~ Alderman Jacobs Primary School ensures that all children in Early Years have a personal 'Learning Journal' which records photos, observations and comments in line with the Early Years Foundation Stage (EYFS) to build up a record of each child's interests and achievements during their time in the EYFS.

Aims:

- To provide an online journal of every child's personal development, to understand their level of achievement, interest and learning styles and then shape their learning experiences for each child reflecting those observations.
- To illustrate children's development progress through the different ages and stages in the EYFS.

Key Roles and Responsibilities:

Each child's class teacher will be responsible for the compilation of children's learning journals. All Early Years practitioners within the setting may contribute observations to children's learning journeys.

Procedures

- Alderman Jacobs Primary School uses a secure online Learning Journal system (Tapestry), allowing staff and parents to access the information via a personal password protected login.
- Staff access allows input of new observations and photos or amendment of existing observations and photos.
- Parent access allows input of new observations and photos or the addition of comments on existing observations and photos – parent logins do not have the necessary permission to edit existing material.
- Observations added to the Tapestry system are moderated by class teachers before being added to the child's Learning Journal.
- Parents logging into the system are only able to see their child's Learning Journal. They can also view group observations which include their child.
- Parents sign an agreement to ensure they will not share or publish any images or observations from their child's Learning Journal on any social networking site to protect images of other children that may appear in any photos contained in their child's Learning Journal.
- The Learning Journal is only begun once the child has started in the school and parents have signed consent forms and completed the email request form.
- In groups observations other children are not referred to by name.
- Tapestry is not used as a general communication between Alderman Jacobs Primary School and home. A child's Learning Journal is a document recording their learning and development and parents may add comments on observations or contribute photos, videos or information about activities they have been doing at home. Parents may contact us through the usual channels for any other day-to-day matters, e.g. absence, lost property etc.

Security

- The Tapestry on-line Learning Journal system is hosted on secure dedicated servers based in the UK.
- Access to information stored on Tapestry can only be gained by personal email address and password.
- Parents can only see their own child's information and are unable to login to view other children's Learning Journals.

Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, AJS will have an annual programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

Children from EYFS to Y6 will have regular internet safety discussions, on a theme and promoting honest discussions about the children's real life experiences.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

The e-Safety Training Programme is as follows:

All pupils – Regular internet safety sessions (recommend 3 per half term) discussing internet safety issues around a half termly theme.

Parents – internet safety FaceBook page 'AJS Internet Safety', safety advice on website, e-safety annual event during e-safety week in February (in this academic year 2018-2019 we have held our session early in October)

Staff – e-safety safeguarding as part of CP annual training, annual PREVENT training, internet safety awareness training annually in Autumn Term.

Links to other policies

Acceptable Use Code of Conduct

Behaviour and Discipline

Early Years Foundation Stage

Safeguarding and Child Protection

Mobile Phone and Camera Use in School

Statutory/<mark>Non-statutory</mark>							
~~Created/~~Reviewed /~~Updated~~		Ratified		Review Frequency	Next Review Date	Signed by	
By	Date	By	Date			Head	Chair
Jenny Smith	Spring 2019	Achievement Committee	16 January 2019	Annually	Spring Term 2020	*Cathy Carlisle*	*Hilland*