ALDERMAN JACOBS PRIMARY SCHOOL (ACADEMY TRUST)

ACCEPTABLE USE CODE OF CONDUCT

Aims

Our school aims to:

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

Definitions

The term **Acceptable Use** is used by the DfE and schools to refer to the manner in which technology and online communication is used.

Roles and Responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing board will co-ordinate regular

meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Trustee who oversees online safety is Laura Hemmaway.

All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

The Headteacher
The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead
Details of the school's Designated Person (DP) for safeguarding are set out in our child protection and safeguarding policy.

The DP takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT Leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board

This list is not intended to be exhaustive.

The ICT Leader
The ICT Leader is responsible for:

- Ensuring appropriate filtering and monitoring systems are in place, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Regularly conducting a full security check and monitoring the school's ICT systems

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DP to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Acceptable Use

Pupils

- Pupils may only log on to the school network using their own username and password, or the 'pupil' log on and password.
- Children will use the Internet for school related work only and with permission from an adult who is responsible for their use. An adult must be in the same room and supervising children on the internet.
- Children should use Google search under supervision only and with the security settings set to the highest possible level.
- Children may only download pictures and sounds with direct supervision and these must be saved in the child's own folder on the network. Children must be made aware of copyright law and expectations when using such material.
- Children should be taught how to organise their own work into folders and be encouraged to delete files that are no longer required.
- Children will be required to use their Google account to save and share work. They are responsible for it's appropriate use and any inappropriate behaviour or language will be dealt with in line with the behaviour policy.
- Any e-safety issues must be dealt with as a Child Protection issue and recorded in the same manner. This can include any unsuitable material accessed or any incidents of cyber bullying, to include the use of mobile phones.
- The production and distribution of sexting images involving anyone under the age of 18 is illegal and incidents of sexting will be investigated in conjunction with our Child Protection and Safeguarding policy and procedures. If a device is involved it will be confiscated and set to flight mode, where possible, or off.
- Children must have mobile phones silent and out of sight when they are on school property, including the field and playground, unless under supervision of an adult – for example sending a message home. Unauthorised use of a phone may lead to confiscation during school hours by the class teacher. Please see separate Mobile Phone policy for further clarification.
- 'Smart' watches and fitness bands are allowed to be worn only if they are not connected to a mobile phone or directly to a mobile network. If the device has a 'camera' feature then it may not be worn in school.
- Reading records/homework diaries that contain log on details to school systems must be kept safe and if lost teachers must inform the ICT leader to have passwords changed.

Staff

- Staff must attend an annual 'e-safety' session to protect themselves and the children in their care.
- Staff are responsible at all times for the internet use on their laptops, i-pads and class computers. They will be held liable for any inappropriate use, including sites accessed away from the school premises.
- Staff should be aware of their own e-safety and fully understand the potential issues relating to personal information posted on the internet, in particular social networking sites. They should only ever use SchoolComms to communicate with pupils or parents.

- Staff must make sure that they 'lock' their laptops whenever they are not present in the room.
- Staff must not use the school network to store personal files, including in particular music, photo and video files.
- Staff must delete all photos and videos of children used for observation purposes and stored in password protected files from their school laptops or i-pads on a monthly basis unless it is deemed necessary to keep them as evidence (eg in EY setting). In which case, photographs that are kept for evidence will be kept on the individual staff members' school laptop; accessed by their own personal log-in, on their C drive and not on a shared drive. The file will be password protected. A diary note will be made and the photograph will be deleted when it is no longer required for evidence.
- Staff may not use mobile phones/cameras in the Early Years/Preschool setting during school hours.
- Any member of staff authorised to access SIMS data through central hosting must ensure that they do not leave laptops unattended at any point when logged onto the system.
- Staff using SIMS or working with any other sensitive data must be also aware of their surroundings, particularly if accessing data away from school and must be mindful of data protection at all times.
- Staff must not save work or data onto any external hard drive or memory stick.
- Staff should ensure that 2 factor authentication is selected when setting up and using ipads.
- Staff must be aware that their school bought devices remain the property of the school and must be returned if required by the school, returned to factory settings and with and passwords removed.
- If staff use their own device to access school information eg emails/gdrive then the device must be password protected. Their school google account must also be set to the highest level of security eg asking for the password on every log in.
- If a staff member loses a personal device or has it stolen, school must be informed immediately so that the relevant school accounts can be removed from the lost device.
- If staff use a personal device to download any attachments, then these must be deleted from the device storage immediately.

Parents

- Parents are encouraged to be aware of potential e-safety dangers and are kept informed through information on the school website, through the facebook page 'AJS Internet Safety', through our annual 'e-safety' sessions & through regular tips in the school newsletter.
- Parents may not use their mobile phones in the Early Years/Preschool setting.
- Parents may only access the Google Classroom with their own child's account but must be aware that they are not permitted to take an active part in the classroom. They must be aware that any information and data on the classroom remains the property of the school and is not for distribution in any way.
- Parents should only contact staff through the official school channels.
- Parents are not expected to post pictures of pupils other than their own children on social networking sites.

- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.
- If parents set up school related social media accounts, they must make it clear that the material posted does not reflect the views of the school or be linked to the school in any way.
- Parents may use their Tapestry log on details for personal use only to inform them of their child's learning journey. They may not share or discuss information or images from the Tapestry site.

Trustees

- Trustees should follow the same guidelines as staff with these additional clarifications
- Trustees' minutes and other documents shared at meetings should be electronically shared only through the official school based email system and not transferred or saved to any personal device.

Links to other policies:

Behaviour & Discipline
Safeguarding and Child Protection
Data Protection & Privacy Notice
E-Safety

Statutory/Non-Statutory							
~~Created/~~Reviewed **~~/Updated~~**		**Ratified**		**Review Frequency**	**Next Review Date**	**Signed by**	
By	**Date**	**By**	**Date**			**Head**	**Chair**
Jenny Smith	Spring Term 2019	Achievement Committee	5 February 2020	Annual	Spring Term 2021	Cathy Carlisle	Helland