The Alderton Junior School

E-SAFETY POLICY

Originator: M. Harrison

Adopted on: September 2020

Revision Date: September 2023

The Alderton Junior School
Alderton Hall Lane
Loughton
IG10 3HE

Telephone: 020 8508 2521
Email: admin@Alderton-jun.essex.sch.uk
Website: www.Alderton-jun.essex.sch.uk

Alderton Junior School E-Safety Policy 2020-23

(Read in conjunction with Safeguarding, Computing, Devices and Social Media Policies)

The main purpose of this policy is to ensure that members of staff, pupils and the wider school community understand the approach Alderton Junior School takes to e-safety and the steps we take to minimise any risks that may be found in the modern world. The curriculum at Alderton Junior School is designed to educate pupils whilst opportunities are given to staff, parents and carers to participate and update their own e-safety awareness.

The E-Safety Policy will be reviewed every three years, or when any significant changes occur with regard to the technologies in use within the school. All staff are responsible for the implementation of this policy.

Aims

- To ensure the school is in line with statutory requirements.
- To give all members of the school community a clear understanding of e-safety.
- To give children and adults the tools to use the internet safely.
- To minimise the risk of children and adults being exposed to inappropriate content on the web.

Internet access, security (virus protection) and filtering

All users at Alderton Junior School are informed that Internet and e-mail use is monitored.

Alderton Junior School has educational filtered secure broadband connectivity through LGFL (London Grid for Learning) and uses the LGFL Webscreen filtering system, which blocks sites that fall into categories (e.g. adult content, hate, gaming).

Alderton Junior School only uses secure clouds (Google Drive) where staff need to access data off-site.

Alderton Junior School continues to work in partnership with LGFL and our technical support provider (Academic IT) to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Pupil e-safety curriculum

A thorough and age appropriate e-safety curriculum is delivered to all pupils at Alderton Junior School to teach children how to stay safe when using computing technology in school or at home (Appendix 1). This covers a range of skills and behaviours appropriate to their experience. The curriculum has been planned out to cover a broad range of e-safety aspects and prepare children for a digital world. The curriculum will review and remind students about their responsibilities through the pupil Acceptable Use Agreement (see Appendix 3).

Across the curriculum, it is ensured that pupils only use school-approved systems and work within appropriately secure and age-appropriate environments.

Training and Induction

Staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, for example the use of passwords, logging-off, use of content, research skills, copyright; this is updated through staff training.

Alderton Junior School makes regular training available to staff on e-safety issues and the school's e-safety education programme. It also provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the E-Safety Policy and the school's Acceptable Use Agreements. In addition, training and/or induction is provided for all governors, student teachers and regular visitors, such as outside agencies.

All adults at Alderton Junior School should be vigilant in the supervision of children at all times, as far as is reasonable, and use common-sense strategies in learning resource areas, where older pupils have more flexible access; know to take professional, reasonable precautions when working with pupils, previewing websites before use; using guided, age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

This policy is part of the school induction pack for new staff. Acceptable Use Agreements will be digitally issued to the whole school community on joining the school, as well as at the start of each academic year, and must be signed in accordance with this policy. (See Appendix 2).

Online Safety Group

An Online Safety group (including staff, governors and parents) has been formed to ensure the implementation of the E-Safety Policy and to review any online safety concerns and incidents. The group meets on a yearly basis to review policies, incidents and the latest developments.

This group will also monitor the Alderton Junior School Privacy Notice.

Parents/Carers

Parents and Carers are asked to provide consent for pupils to use the Internet, as well as other technologies, when their child is admitted to the school.

Parents and Carers should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse as stated below. These form the pupil's Acceptable Usage Agreement.

Alderton Junior School provides E-Safety Workshops for parents, which includes online safety and runs a rolling programme of e-safety advice, guidance and training for parents.

E-Safety Concerns & Incidents

The school will take all reasonable precautions to ensure online safety. Staff and pupils are given information about infringements and possible sanctions. The Technology Leader acts as a first point of contact for any incident, which should be reported as soon as possible. Any concern about staff misuse is always referred to the SLT, unless the concern is about the Headteacher or SLT, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). For more information, see below.

At Alderton Junior School, there is strict monitoring and application of the E-safety Policy and a differentiated and appropriate range of sanctions.

All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

Appendix 4 further expands on possible e-safety scenarios and the escalation process. An E-Safety Log (Appendix 5) will be completed for incidents ranked at green and above on our system. Parents/carers are specifically informed of e-safety incidents involving young people, for whom they are responsible; the police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law; support is actively sought from other agencies as needed (i.e. the local authority, Essex School Broadband Service, UK Safer Internet Centre helpline, Child Exploitation and Online Protection, Prevent Officer, Police, Internet Watch Foundation) in dealing with e-safety issues.

We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA. Monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school.

Network Management (user access, backup)

Alderton Junior School uses individual, audited log-ins for all users. For external or short term visitors, Alderton Junior School uses guest accounts for temporary access to appropriate services.

Alderton Junior School uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful.

Where appropriate, Alderton Junior School has additional local network monitoring/auditing software installed.

Alderton Junior School's Technical Support Provider must ensure they keep up-to-date with local and national authority services and all relevant school policies.

Alderton Junior School uses secure, 'Cloud' storage for data back-up that conforms to General Data Protection Regulation (GDPR) compliance. The storage of all data within the school and online data linked to the school will conform to the EU and UK data protection requirements.

To ensure the network is used safely, Alderton Junior School:

- Ensures staff read and sign that they have understood the school's Acceptable Use Policy. Following this, they are set-up with Internet, e-mail access and network access. Access to the school network and online service is through a unique, audited username and password.
- Pupils should never be allowed to log-on to or use teacher and staff logins or devices.
- During school, it is required all users log off when they have finished working or are leaving any school device unattended.
- Alderton Junior School, where appropriate, ensures all equipment owned by the school has up to date virus protection.
- This policy makes clear that staff are responsible for ensuring any laptop or mobile device loaned to them by the school, is only used to support their professional responsibilities. It also makes clear that children using technology in their provision are their responsibility.
- Alderton Junior School ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through the school approved system. It does not allow any outside agencies to access our network remotely, except where there is a clear professional need.
- The wireless network has been secured to industry standard security level and follows appropriate standards suitable for educational use.

Password policy

This school makes it clear that staff and pupils must always keep their passwords private, must not share with others. If a password is compromised the school should be notified immediately. All staff have their own unique username and individual passwords to access school systems. Staff are responsible for keeping their password(s) private, unless required by administration purposes.

In the case of shared systems, such as cloud storage, logins and passwords may be shared with those who need access to specific accounts. If a member of staff is unsure of how to proceed, they should contact the Technology Leader.

E-mail

Alderton Junior School provides staff with an email account for their professional use. Staff should not use their personal email addresses for school correspondence. At present, we use a number of Essex country approved technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Alderton Junior School will contact the police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.

Staff should never use email to transfer staff or pupil personal data. Staff should use professional judgement when sending school related documents, even to share with colleagues.

There is no requirement for students to have personalised school emails.

School website

The Headteacher, supported by the Governing Board and selected members of staff, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school website complies with statutory DfE requirements.

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.

Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Social networking

Staff are instructed to always keep professional and private communication separate. Teachers are instructed not to run social network sites as a means of communication with students or parents. School staff should not be on-line friends with any pupil/student. Any exceptions must be approved by the Headteacher.

In private use, staff will ensure no reference should be made in social media to pupils, parents/carers or school staff. Staff do not engage in online discussion on personal matters relating to members of the school

community. Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.

Security settings on staff's personal social media profiles should be regularly checked to minimise risk of loss of personal information and to ensure content that is public, is appropriate.

Alderton Junior School uses Social Networking to update parents and carers and as a running news feed. Parents and carers are given the opportunity to opt out of their children appearing in such media via the school's Photography and Video Consent Form.

Pupils are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our e-safety curriculum work. Pupils are required to sign and follow our pupil Acceptable Use Agreement. Pupils are deterred from using Social Media until they reach the legal age of requirement.

Parents are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Cloud Environments

Uploading of information on the school's online learning space (Google Suites) is shared between different staff members according to their responsibilities, e.g. all class teachers upload information in their class areas; documents uploaded to the school's online environment will only be accessible by members of the school community and are solely related to children's work.

In school, pupils are only able to upload and publish within school approved 'Cloud' systems to save any school related documents.

Staff are prohibited from using any USBs, external hard drives or personal cloud storage as this can cause a risk to the system or transfer sensitive data. All staff have access to school based cloud systems which can be used to transfer appropriate data and information securely.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission, unless required to do so by law.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the school staff and is not used for any other purposes.

Strategic and operational practices

At Alderton Junior School, the Head Teacher is the Senior Information Risk Officer (SIRO).

Staff are aware of the key contact(s) for key school information (the Information Asset Owners). We have listed the information and information asset owners. All staff, volunteers and governors are required to sign the schools AUP agreement annually.

We ensure staff know who to report any incidents, where data protection may have been compromised.

All staff, governors, volunteers and regular outside agency staff are DBS checked and records are held in a Single Central Record.

Technical Solutions

Staff are only provided with access to authorised areas of the school network through their unique user ID and password to the school network. Alderton Junior School requires staff to log-out of systems when leaving their computer.

All servers are in lockable locations and managed by DBS-checked staff.

Details of all school-owned hardware are recorded on the school's asset register. Software is monitored across devices to ensure that it is in line with school policies.

ICT equipment will only be disposed of or recycled when hard drives are wiped clear of all school data.

Privacy Notice

The Alderton Junior School has a Privacy Notice available on the school website. This outlines GDPR procedure and the information the school shares with various companies.

Mobile Devices

The mobile devices sections forms a part of the e-safety policy which must be adhered to and is set out as an extension to the main policy.

This policy defines 'Mobile Devices' as, but not exclusively:

- Mobile Phones
- Smart Phones
- Video Cameras
- Still Cameras
- Tablets
- Any device with a recording function / camera

Aims

- To set out what is 'acceptable' and 'unacceptable' use of mobile devices by the whole school community (children, staff, student teachers, governors, volunteers, regular outside agency staff and visitors) while they are at School or undertaking school activities away from school.
- To protect an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.
- To prevent unacceptable use of mobile devices by the school community, and thereby to protect the school's staff and children from undesirable materials, filming, intimidation or harassment.

This Policy is categorised into four main areas – General issues; the use of mobile devices by children; the use of mobile devices by staff; and the use of mobile devices by parents, carers and other adults.

General Issues

Mobile devices are brought into school at the risk of the owner. The School accepts no responsibility for the loss, theft or damage of any mobile device brought into school.

The School reserves the right to search the content of any mobile device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Staff personal mobile phones will not be used during working hours except during designated break times, although this should not be in the presence of children. If a staff member is expecting an emergency call should seek specific permissions to use their phone at a time other than their break times from a member of SLT.

Under no circumstance should images or videos be taken on any personally-owned mobile devices.

A Social Media policy is also in place and further outlines the roles and responsibilities of all staff.

The use of mobile devices by children

Children's personally-owned devices must be handed in to the school office.

The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. However, the School strongly discourages children bringing in mobile devices unless absolutely necessary.

If a child breaches this policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will only be released to parents or carers, in these circumstances and will not be given back to the child.

If a child needs to contact his or her parents or carers, they will be allowed to use a school's landline if it is deemed necessary.

The use of mobile devices by Staff

Staff are not permitted to use their own mobile devices for contacting Alderton Junior children, young people or their families within or outside of the setting in a professional capacity.

Each classroom has an iPad which is allocated. These devices can be used to take photos of work including children who have consent from a parent or carer. These devices cannot leave the school site.Staff will be provided with mobile devices, as the school deems necessary, in order to deliver the majority of their role. Personally owned mobile devices should not be used as part of teaching and learning. Staff devices use encryption and advanced passwords.

Staff will be issued with a school mobile phone where contact with children, parents or carers is required such as on school trips. A school mobile device is available from the school office and should be used on all school trips.

Mobile devices should be switched off or switched to 'silent' mode. Any external communication systems should be 'hidden' or switched off and mobile phones or personally-owned devices should not be used during teaching periods, unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.

Personally owned mobile devices should not automatically synchronise with any school endorsed system. In the case of a personal device accessing school email, members of staff should ensure that appropriate steps are in place to protect personal data by using secure pin codes or passwords. Failure to do so could result in disciplinary action, a breach notification and/or a fine imposed under General Data Protection Regulation.

Staff should not use personally owned mobile devices to take photos or videos of children in any circumstance and should only use work-provided equipment for this purpose.

In an emergency where a staff member does not have access to a school-owned mobile device, they can use their personally owned mobile device and hide (by inputting 141) their own mobile number for confidentiality purposes.

On an annual basis, all staff sign an Acceptable Use Policy that covers the use of mobile devices at a more in depth level. Failure to comply with the school's AUP could result in disciplinary action.

The use of mobile devices by Parents, Carers and other adults

When in the school building, parents, carers and other adults are prohibited from using mobile devices. Once in the school building, mobile devices should be on silent or switched off.

If a parent or carer needs to contact their child, they are advised to phone the main school number between 8.30am and 4.00pm.

Parents may be given consent to take photographs and videos of their children in situations such as Family Assemblies and Sports Day. However, a member of staff will give permission prior to the event, if allowed to do so. Under no circumstance should these images be posted on social media as they may include children whose parents have refused consent for images to be used on these platforms.

App. 1 - E-Safety Curriculum and Useful Links

E-Safety Curriculum 2018/2019
ES- ESafety; DL-Digital Literacy

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Year 3	E-Safety basics – what is SMART thinking?	To understand how we handle unwanted content (DL)	To understand what responsible technology use is (DL)	To understand how to use the services the web provides through search engines such as Google (DL)	To understand how to get help and using the SMART steps	To recognise whether technology always achieves my goals
Year 4	E-Safety basics – how can we remember to think SMART?	To explore our own e-safety concerns	To recognise acceptable behaviour using technology (DL)	To recognise unacceptable behaviour using technology (DL)	To understand what safe searching on the web is	To identify and select correct information
Year 5	E-Safety basics – when does SMART apply?	To understand what personal information we share (DL)	To recognise how we make choices on the web and the potential effects they can have (DL)	To recognise that not everything is true/safe and what ranked results are (IT/DL)	To understand what Safe communicatin g is	To understand when to report on sites we use (other medias)
Year 6	E-Safety basics – chn's knowledge	To explore the importance of acting our age online	To recognise online risks and what can be done to avoid them (DL)	To recognise how we leave a digital footprint (DL)	To understand what copyright is and how it applies to online searching	To understand how we can stay safe on Social Media

The following resources can be used as a tool to support E-Safety lesson plans:

BBC Bitesize - http://www.bbc.co.uk/education/topics/zcpp34j/resources/1

ChildNet Resources - http://www.childnet.com/resources

ThinkUKnow – http://www.thinkuknow.co.uk/

Google Legends - http://www.google.co.uk/safetycenter/families/legends/downloads-resources/

LGfL Resource Matrix - http://www.lgfl.net/esafety/Pages/Primary-resource-matrix.aspx

Childnet (Information for you)
https://www.childnet.com/teachers-and-professionals/for-working-with-young-people/hot-topics

E-Safety News https://www.e-safetysupport.com/newslinks/latest

E-Safety quiz https://www.o2.co.uk/help/nspcc/parents-vs-kids/play#/quiz

Year 3 resource ideas & additional information:

1. E-Safety basics – what is SMART thinking? - http://www.kidsmart.org.uk/beingsmart/
2. To understand how we handle unwanted content (DL) - https://www.thinkuknow.co.uk/professionals/resources/play-like-share - includes videos and information
3. To understand what responsible technology use is (DL) - What do we do **(as a user)** to be safe & responsible with technology? / Chicken Clickin' Book

4. To understand how to use the services the web provides through search engines such as Google (DL) - using https://www.safesearchkids.com/google-kids/#.XOOzQCBKgdU and understanding how to word our searches - e.g. going from searching for 'Saxons' to 'Sutton Hoo information for kids'
5. To understand how to get help and using the SMART steps - https://www.bbc.co.uk/programmes/p025lqs5
6. To recognise whether technology always achieves my goals - debate ideas around the use of e-safety / Scenario cards / circle time: e.g. 'To find information about Italy'/'To have quality time with friends'

Year 4 resource ideas & additional information:

1. E-Safety basics – how can we remember to think SMART? - http://www.kidsmart.org.uk/beingsmart/ -
2. To explore our own e-safety concerns - https://www.bbc.co.uk/newsround/13910067
3. To recognise acceptable behaviour using technology (DL) - https://www.bbc.com/bitesize/clips/z9rw7ty
4. To recognise unacceptable behaviour using technology (DL) - https://www.stem.org.uk/resources/elibrary/resource/362331/e-safety-scenario-cards
5. To understand what safe searching on the web is - ext with ideas about ranked results: https://www.bbc.com/bitesize/clips/zspbcdm
6. To identify and select correct information - https://www.bbc.com/bitesize/clips/zw8mtfr / http://clairelotriet.com/blog/2015/01/25/evaluating-digital-content-6-resources-for-teachers/

Year 5 resource ideas & additional information:

1. E-Safety basics – when does SMART apply? - http://www.kidsmart.org.uk/beingsmart/
2. To understand what personal information we share - https://www.stem.org.uk/resources/elibrary/resource/362346/personal-information (use resources to create 1 lesson)
3. To recognise how we make choices on the web and the potential effects they can have (DL) - https://www.vodafone.co.uk/mobile/digital-parenting/goldilocks
4. To recognise that not everything is true/safe and what ranked results are (IT/DL) - https://www.bbc.com/bitesize/articles/zt9thyc / https://zapatopi.net/treeoctopus/ (fake website - Wikipedia even has an entry explaining it)
5. To understand what Safe communicating is - https://www.bbc.com/bitesize/articles/z9r72hv#zyf8d2p
6. To understand when to report on sites we use (other medias) - https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Year 6 resource ideas & additional information:

1. E-Safety basics – chn's knowledge - http://www.kidsmart.org.uk/beingsmart/
2. To explore the importance of acting our age online - https://www.tes.com/teaching-resource/act-your-age-online-safety-animated-story-ks2-e-safety-social-media-facebook-11218299
3. To recognise digital risks and what can be done to avoid them (DL) - https://www.youtube.com/watch?v=XwuKz4kyDRI
4. To recognise how we leave digital footprints (DL) - https://www.bbc.com/ownit/its-personal/digital-footprint-quiz
5. To understand what copyright is and how it applies to online searching - https://www.bbc.co.uk/copyrightaware/what-is
6. To understand how we can stay safe on Social Media - https://www.bbc.com/ownit/its-personal/mandeville-sisters-stolen-images?collection=be-body-kind / https://swgfl.org.uk/online-safety/resources/social-media-checklists/snapchat-checklist/ / https://swgfl.org.uk/online-safety/resources/social-media-checklists/instagram-checklist/ / use a template to create a safe online profile

Bonus links and resources:
https://static.lgfl.net/LgflNet/downloads/online-safety/LGfL-OS-Pupil-scenario-discussion-cards.pdf

Appendix. 2 Staff Acceptable Use Policy

The Alderton Junior School Acceptable Usage Policy	
AUP review Date	**September 2019**
Date of next Review	**September 2020**

Who reviewed this AUP?	Technology Leader

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will follow the E-Safety, Devices, Computing and Social Media Policies.
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Board.
- I will not reveal my password(s) to anyone, this includes personal devices where used to access school data.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it and report it immediately to the appropriate member of staff.
- I will not allow unauthorised individuals to access my school email address / the Internet / the school network, or other school systems, or any Local Authority (LA) system I have access to without the Headteacher's prior consent.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's IT Security Policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: *Outlook 365 Essex StaffMail*
- I will only use *school approved communication systems* with pupils or parents/carers, and only communicate with them on appropriate school business. For more details, read the Devices Policy.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Technology Leader, Technology Impact Team or School Business Manager.
- I will not download any software or resources from the Internet without the prior consent of the Technology Leader who will conduct a Data Protection Impact Assessment prior to approving the software/resources.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not use USBs, personal clouds or any other storage devices in school. If access to work related content is required, then I will use either remote access or school provided cloud systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos on personal devices or at home.
- I will only use school approved equipment, networks or cloud systems for storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.
- I will only access school resources remotely using the school approved systems.

- I understand that the General Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert Alderton Junior School's Technology Leader and/or Child Protection Officer / appropriate senior member of staff if I feel the behaviour of any user of the school's IT systems may be a cause for concern.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Headteacher / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only:* I will embed the school's e-safety policy and computing policy into my teaching.

Alderton Junior School
Acceptable Use Policy (AUP): Agreement Form
All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent E-Safety, Devices, Computing, IT Security and Social Media Policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: Date:

Full Name: (printed)

Job title / Role:

Authorised Signature (Head Teacher / Deputy / Technology Leader)

I approve this user to be set-up on the school systems relevant to their role.

Signature: Date:

Full Name: (printed)

Appendix 3

User Agreement 2019

Alderton Junior School KS2 Acceptable Use Policy 2019

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will use the school's computers and equipment sensibly. Look after it and make sure it is stored securely when I have finished using it.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

Appendix 4 – Alderton Junior School's Levels of E-Safety and Escalation Process

Category 1	Category 2	Category 3	Category 4	Category 5
Staff dealing with incident:	**Staff dealing with incident:**	**Staff dealing with incident:**	**Staff dealing with incident:**	Staff dealing with incident: SLT/Head

Staff reporting incident **Informing:** Class teacher Computing and E-Safety Lead	Computing and E-Safety Lead Class teacher **Informing:** Head of Year	Computing and E-Safety Lead Head of Year/SLT **Informing:** SLT	Computing and E-Safety Lead SLT/Head **Informing:** Head/Governors	Governors Computing and E-Safety Lead **Informing:** Local Authority
Pupil related incident. **Example of incident:** Accidentally viewing image through safe search that has upset the child but not deemed to be inappropriate.	**Pupil related incident.** **Example of incident:** Accidentally viewing image through safe search that should not have gotten through filtering (e.g. nudity)	**Pupil related incident.** **Example of incident:** Sharing personal information. Cyberbullying**.**	**Pupil related incident.** **Example of incident:** Sharing and/or distributing inappropriate content. Repeated cyberbullying.	**Pupil related incident.** **Example of incident:** Seeking out inappropriate content such as pornography, terrorism, etc.
Staff related incident. **Example of incident:** Concerns over own Social Networking sites security	**Staff related incident.** **Example of incident:** Concern over messages received on school based social networking	**Staff related incident.** **Example of incident:** Contacting parents/carers with personal devices.	**Staff related incident.** **Example of incident:** Sharing of content between children and staff outside of school settings.	**Staff related incident.** **Example of incident:** Sharing of inappropriate content between children and staff.
		Parent/Carer related incident. **Example of incident:** Parents allowing students to use social media.	**Parent/Carer related incident.** **Example of incident:** Parents allowing students to be exposed to inappropriate age-rated content (e.g. games/films).	**Parent/Carer related incident.** **Example of incident:** Exposing children to inappropriate content such as pornography, terrorism etc.

All concerns can move up the scale depending on circumstances and urgency. Computing and E-Safety Leader should be first point of call for **ALL** incidents and will relay information to the appropriate members of staff once an outline of events has been established. Any e-safety issue identified as green or above must identified in an e-safety log.

A full, detailed Escalation Process is also available.

Appendix 5 E-Safety Log

E-Safety Incident Log

Details of **ALL** e-safety incidents, green or above, to be recorded by the Computing and E-Safety Leader, Alderton Junior School's Technical Support or any other appropriate member of staff. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors.

Date & Time	Name of pupil or staff member	Room and computer / device number Actions	Name and role of person completing this entry
19/3/21	Summer		M Harrison

Details of incident (including evidence)	Actions

Details of first reviewing person (person reporting incident):

Name	
Position	
Signature	

Website(s) address / device	Reason for concern

Follow up action (if required)/Outcome:
