E-safety Policy

Policy Title:	E-safety Policy
Version:	March 2021
Trust Board Approval:	
Date of Next Review:	March 2022

Index

1. Introduction

New technologies have become integral to the lives of children and young people in Society. The internet and other digital and information technologies are powerful tools, which open up new learning opportunities for everyone.

Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. However, it is vital Children and young people should have an entitlement to safe internet access at all times. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools and academies are bound.

Aldridge Education E-safety policy will help to ensure safe and appropriate use. The development and implementation of the policy will involve all the stakeholders in a child's education from the CEO, Trust Team, Principals and Designated Safeguarding Leads to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the academy's sites. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Currently the internet technologies children and young people are using both inside and outside of the classroom or school environment include:

- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging apps.
- Chat Rooms and social networking sites

- Blogs and Wikis
- Podcasts, audio sharing.
- Phone apps
- Video sharing, video conferencing and/or broadcasting
- Music streaming and/or downloading
- Gaming and virtual worlds.
- Mobile/Smart phones with SMS, apps, video and/or web functionality
- Other mobile devices with web functionality.

As part of our commitment to learning and achievement Aldridge Education Academy Trust want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement
- Develop the curriculum and make learning exciting and purposeful
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security
- Enhance and enrich their lives and understanding.

To enable this to happen we have taken a whole Trust approach to E-safety. This includes:

- The development of policies and practices
- The education and training of staff and pupils and
- The effective use of the Trust IT infrastructure and technologies.

Aldridge Education Academy Trust has developed an E-safety yearly programme to ensure our digital users (Trustees, Trust leadership team, school leaders, local governors, staff, students, parents and our communities) are fully aware and properly supported when using any ubiquitous Internet connected devices.

As a Multi Academy Trust we are committed to make Internet secure, ensuring that all Information Technology users are educated as to the risks that exists when using the Internet and that themselves can take an active part of promoting a safe Internet environment.

2. Purpose

- It takes into account the DfE statutory guidance Keeping Children Safe in Education, Early Years and Foundation Stage and the inspecting E-safety by Ofsted.
- The purpose of this E-safety policy is to:
    - Safeguard and protect all members of Aldridge Education online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.

- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

- Aldridge Education identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

- Aldridge Education will ensure that through the Trust yearly E-safety Programme we have the elements in place to enrich, safeguard and empower all IT Internet users.

- Here is an example of elements that are included in our E-safety Programme each year:

- E-safety training for senior leaders, staff, students, parents, and school communities.
- A range of IT and related policies are frequently reviewed and updated.
- Supervision, monitoring and filtering of pupils when using the Internet and digital technologies in all organisational devices.
- E-safety embed into the curriculum that is aimed at ensuring safe use of Internet and digital technologies.
- A robust monitoring, auditing and reporting procedures for abuse and misuse.
- Information to parents and community that highlights safe practice for children and young people when using the Internet and other digital technologies.
- A complete audit of each year E-safety programme is in place. This enables us to improve on our practices and make sure that our programme is up to date and current with the latest technologies/topics and it is engaging for all stakeholders every year.

3. Roles and Responsibilities

3.1 Principals

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy *and/or* acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.

- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

3.2 Designated Safeguarding Leads (DSL)

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside senior leaders and pastoral teams to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns in line with Aldridge Education child protection and safeguarding policies and procedures.
- Work with the Trust leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with Director of IT and Trust Lead for Inclusion to lead responsibility for safeguarding and/or online safety.

3.3 Staff members

- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site. This includes using Aldridge Education services and infrastructure using personal devices (Bring Your Own Device, BYOD).

- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Staff should not give access to usernames, passwords, or devices to anyone else.

3.4 Technical Team

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate technology security measures to ensure that the IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the settings Internet Service Provider or other filtering and monitoring services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the safeguarding procedures.

3.5 Learners

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.
- Learners also include any adult learners onsite, remote learning or apprentices.
- Learners should not give access to usernames, passwords, or devices to anyone else.

3.6 Parents and carers

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the e-safety and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.

- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

3.6 LGC and Trustee safeguarding leads

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy *and/or* acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the Principal by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensuring that E-safety programme is being implemented successfully.
- The named LGC and Trustee safeguarding lead will report on a regular basis to the Governing/Trustee Board on online safety practice and incidents, including outcomes as part of the safeguarding process and policy. Please refer to the Trust Model Safeguarding and Child Protection policy and each school's own Safeguarding and Child Protection policy for more information.

4. Safe Use of Our Technology and Services

4.1 Classroom Use

- Aldridge Education uses a wide range of technology. This includes access to:
    - Computers, laptops, Chromebooks, tablets, and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platforms, intranet sites like Google Apps for Education or Microsoft 365.
    - Internet collaboration tools, email, internal communication chat-based platforms.
    - Games consoles and other games-based learning technologies.
    - Digital cameras, web cams and video cameras
- All setting for organisational devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- Staff will use age appropriate search tools following an informed risk assessment or change request, to identify which tool best suits the needs of our students.
- We will ensure that the use of internet-derived materials, by staff and learners complies with current copyright and data protection laws and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.

    - Early Years Foundation Stage and Key Stage 1
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
    - Key Stage 2
        - Learners will use age-appropriate search engines and online tools.
        - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.
    - Key Stage 3, 4, 5
        - Learners will be appropriately supervised when using technology, according to their ability and understanding.

4.2 Managing internet access

- We will maintain a record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

4.3 Filtering and Monitoring

- We have based our filtering and monitoring settings based on guidance from our filtering and monitoring technology partners and UK safer Internet Centre documentation on establishing 'appropriate levels' of filtering and monitoring: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

4.4 Decision Making

- Aldridge Education will ensure that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The Trustees and leaders at Aldridge Education are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed through change requests by staff with educational and technical experience and, where appropriate, with consent from the Trust leadership team; all changes to the filtering policy are logged and recorded.

- The Trust and local leadership teams will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

4.5 Filtering

- Aldridge Education academies have filtering systems which block sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature, etc.
- The filtering system blocks all sites per categories and type of user group.
- Aldridge Education academies provide filtering and monitoring to all organisational devices as well as guests' devices and any other personal devices (Bring Your Own Device) connected to academy site BYOD internet services.
- We work with our filtering technology partners and suppliers to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Turn off monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL and/or technical staff through the IT helpdesk.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police or CEOP.

4.6 Monitoring

- Aldridge Education will appropriately monitor internet use on all organisational devices provided and through special BYOD access to our internet services. This is achieved by:
    - Physical monitoring (supervision)
    - Monitoring internet and web access (reviewing logfile information)
    - Live technology monitoring services through our filtering, logs and firewalls.
    - Daily/Weekly alert review of positives and false positives alerts.
    - Monthly report reviews and analysis of trends and behaviours.
- If a concern is identified via monitoring approaches:
    - DSL and staff members will respond in line with the child protection and safeguarding policies and procedures.
    - Raise a Change Request when appropriate to block or allow certain URLs or filtering categories. Any member of staff can submit a Change Request with the school IT helpdesk by email or phone. This request will be reviewed by the IT Cluster Manager, DSL and Director of IT as appropriate considering the nature and urgency of the issue. Any safeguarding concerns will be dealt with immediately.
- All users are informed that all use of Aldridge Education systems and services are monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

- Monitoring and filtering measures does also include guest access and BYOD services provided by Aldridge Education.
- All Trust devices have monitoring software installed. Devices will be monitored at all times independent of the location or internet provider. This software monitoring all internet activity in the devices regardless of the user.
- For Chromebooks, the monitoring is based on user, regardless of Chromebook used (organisational owned or personal). For the rest of the devices, monitoring is based on device, so personal devices are not affected.
- All filtering and monitoring is captured in real-time automatically, sending all potential risks through to the DSLs and Principal. The filtering is auto pre-graded 24/7 through our technology safeguarding partner which will review all alerts and contact safeguarding teams in each site. The alert notifications are sent in real-time by phone, email, and stored within the safeguarding portal available for the relevant site.

  - **Security**

Aldridge Education takes appropriate steps to ensure the security of our IT systems, including:

  - Virus protection being updated regularly.
  - Encryption for all personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files, permissions and sharing settings held on our network and organisational cloud managed environments.
  - The appropriate use of user logins and passwords to access our network.
  - All users are expected to log off or lock their screens/devices if systems are unattended and appropriate timeouts have been setup.
  - Further information about technical environment safety and security can be found at the IT Security Policy.
  - All users will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
  - We require all users to use strong passwords for access into our system and some will require 2 factors of authentication for security reasons.
  - We will post appropriate information about safeguarding, including online safety, on our school websites for members of the community. The E-safety officer on each school will audit and update each year the information provided in line with the Trust E-safety yearly programme.

  - **Images and Videos**

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

- **Email and electronic communication**

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

  - The forwarding of any chain messages/emails is not used before previously check content and recipients.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email or platform.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

- Members of the community will immediately inform the IT team or DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.
- We will have a dedicated email for anonymously reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- The use of personal email addresses by staff for any official setting business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.
- Learners (when appropriate) will use provided email accounts for educational purposes.
- Learners (and/or carers) will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- All email communication should have the appropriate organisational signatures, updated role, and contact information.

- **Video conferencing and remote live learning**

- Aldridge Education recognise that videoconferencing *and/or* use of webcams can be a challenging activity but brings a wide range of learning benefits.
- All videoconferencing *and/or* webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Videoconferencing contact details will not be posted publicly.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure. Staff must only use Aldridge Trust approved video conferencing software and services.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.
- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability. It will only take place via officially approved school communication channels and platforms.

- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.
- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

    - **Student guidelines and expectations for live remote teaching**
- Remote learning can be a great way to continue learning outside the classroom, particularly in difficult circumstances.
- For students, it's the perfect way to ensure they still get the education they need, despite not being at school. However, it
- also requires a level of discipline and careful planning. That's why we've created this guide to help pupils understand
- different aspects of remote learning and to support them in ensuring their experience is as safe and secure as it can be.

- Guidance and expectations for students:
- Treat remote learning the same as classroom learning - Despite being at home, it's important to remember the same rules apply as being in the classroom, particularly in respect of behaviour and conduct. Focus on learning and don't get distracted by your surroundings.
- Use classrooms language - If you are encouraged to communicate through emails and online messages, don't use shorthand text speak and write as though you would speak in class. Remember to be respectful and polite and avoid positing negative comments or spamming the chat.
- Take regular breaks - Whilst remote learning might be an exciting experience to begin with, having prolonged periods of time in front of a screen isn't always healthy. Remember to have regular screen breaks where possible and in your spare time, try to get some fresh air and enjoy other activities away from electronic devices.
- Always conduct video learning in an open space at home – Try to set up the right environment around you at home in an open space so parents can supervise if necessary. Avoid bedrooms as this could be considered inappropriate.
- Only communicate through approve school portals and platforms.
- Stick to teacher rules and guidelines around online learning.
- Dress in school uniform or appropriate attire, and avoid wearing anything too casual as this could deemed inappropriate for school.
- Do not share passwords or other sensitive information.

- Do not use school platforms to discuss personal matters – It is important that you keep school communication channels separate from you own personal communication with friends and family. – if you are worried or concerned about something and wish to speak to a member of staff, please email your class teacher who will arrange for the DSL to contact you.
- Do not share any personal images, videos or links via official school apps and platforms that aren't associated with your learning.
- Look after your mental health and wellbeing – Remove learning ultimately means working alone and missing out on daily social interaction with your friends. IF you ever feel frustrated, low or sad, it's important to discuss how you feel with your parents or your teacher. Keeping in touch with friends over the phone or on social media can also help to keep your spirits up.
- If any students have any concerns or would like to share any issues regarding safety online, please contact your teacher or Designated Safeguarding Lead.

    - **Staff guidelines and expectations for live remote teaching**

- Staff will familiarise themselves with the relevant policies around safeguarding, acceptable use, data protection, student behaviour and online conduct guidelines.
- Consider your surroundings when using video and live streaming, ensuring the positioning of any cameras, background and personal information are not on display.
- Staff will only use school approved platforms and communication channels. Staff will maintain appropriate dress code at all times.
- Staff will distribute a class timetable/schedule for remote learning well in advance. This will help to maintain a structure and lesson plan to classes. Include the frequency of lessons, duration, how they will be delivered, times for online and online learning and any links. This will give parents a sense of structure and reassurance around lesson delivery.
- Staff will ensure the use correct and appropriate technology according to Aldridge Education guidelines and organisational approved platforms and software.
- Staff will protect personal data at all times. Only use appropriate systems and software that require email and password login and to only use school-provided email addresses.
- Consider the needs of SEND pupils and vulnerable learners. It's important to try and accommodate all students, including children with SEND or those who are more vulnerable, and consider different levels of learning.
- Try to make lessons fun and engaging and encourage regular feedback. Remote learning is a fantastic way to be imaginative with teaching and learning and a great way to encourage independent thinking. Try to encourage a two-way flow of communication with parents and students to help maintain transparency and confidence in the learning process.

4.11 E-safety outside the school network environment

- The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their Online Safety Policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The

policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

- The school might impose disciplinary penalties for inappropriate behaviour which include Incidents of cyber-bullying, or other Online Safety incidents covered by this policy, as well as their behaviour and safeguarding policies, which may take place outside of the school, but are linked to students and staff of the school, or where there is evidence that the behaviour could be deemed as bringing the school into disrepute

- As a school we make sure that our students and staff have the knowledge, tools, processes and training necessary to deal with any e-safety incidents in a restricted or unrestricted Internet environment. Promoting a safe use of Internet technologies in a ubiquitous way.

4.12 Reducing online risks

- Aldridge education recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches as part of our Trust wide E-safety yearly programme.

4.13 Social Media

Introduction and basic guidelines from our Social Media policy

- The Internet provides ready access to online spaces and social networking sites which allow individuals to publish un-moderated content. Social networking sites such as Facebook, Twitter, Chat Rooms, Online Gaming Platforms and Instant Messaging can connect individuals to groups of people which may be friends in the 'virtual' world but who may have never met each other in the real world. Users can be invited to join groups and leave comments over which there may be limited or no control.
- Children / young people will be encouraged to consider the associated risks and dangers related to sending or accepting friend requests and posting personal comments, inappropriate images or videos about themselves or their peers and the subsequent difficulty in removing an inappropriate image or information once published. They will also be advised not to publish

detailed private thoughts or emotions which could be considered threatening, intimidating or hurtful to others.

- Children / young people will also be encouraged to never give out any personal details or images which may identify
- themselves, their peers, their siblings / foster siblings, their location or any groups, schools or organisations they attend or
- associate with. This includes real names, dates of birth, address, phone numbers, e-mail addresses, photographs or videos,
- school attended, IM and email addresses, including those of friends, family / foster family and peers. This also includes any 'gangs' they may be affiliated with.
- Children / young people will be advised about e-security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They will be encouraged to invite known friends only and deny access to others by making their profiles private and only accept friend requests from those already known to them.
- Professionals working or in a position of trust with children / young people (including volunteers) must also familiarise themselves about the risks and inappropriateness of sharing personal information about themselves via social networking sites which could be accessed by children / young people and their parents/carers. They will be made aware that any inappropriate material posted could affect their professional status, and role within the school.
- Staff must responsibly restrict access to who can access their social media profiles, and should consider only allowing their friends and family only, and should not accept 'friend requests' by a young person who is still studying at the school.
- Staff must also steer clear of social networking sites that young people are known to frequent except in certain roles.

Expectations:

- The expectations' regarding safe and responsible use of social media applies to all staff, students and members of our communities.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All the Trust IT users are expected to engage in social media in a positive, safe and responsible manner.
    - All IT users at Aldridge Education are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
    - The use of social media during working hours for personal use *is not* permitted.
    - Inappropriate or excessive use of social media by any user during school hours may result in disciplinary or legal action and/or removal of internet facilities. –if used on Trust devices or personal devices and/or if the use is/has impacted on the staff members capability to fulfil their role.

- Concerns regarding the online conduct of any member of Aldridge Education communities on social media, should be reported to the DSLs and will be managed in accordance with our anti-bullying, safeguarding, allegations against staff, behaviour and child protection policies. If the staff member is not satisfied with any action taken and they feel it is right to take the matter outside of their academy, they can contact the Trust CEO and if not satisfied they can contact the Aldridge Education Trustees.

For more information on Social Media please refer to our Social Media policy here:
http://aldridgeeducation.org/finance-policies-legal-information

5. Education and Training

Aldridge Education E-safety programme focus in all areas of the curriculum and staff are trained each year to make sure they have the knowledge to tackle any e-safety queries, incidents or situation that can arise.

Through the E-safety yearly programme we provide the necessary training, advice, and procedures for all AE technology users to be safe while using the internet. This training will be adapted in line with identified trends and concerns to make sure it is up to date with current guidance.

5.1 Student education and engagement

- Aldridge Education has established and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval, and evaluation.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
    - Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
    - Teaching students to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
    - Students are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
    - Ensuring that children are safe from terrorist and extremist material on the internet.
    - Where students are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit. All equipment in Aldridge

Education has filtering and monitoring technologies so they will always be some restrictions.
    - It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need.

- Aldridge Education supports learners to read and understand the acceptable use policies in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access and around the schools.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology.
    - Implementing appropriate peer education approaches.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable students

- Aldridge Education recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Aldridge Education will ensure that differentiated and ability appropriate online safety education, access, support, and specialist equipment (if required) is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum Aldridge Education will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher, DSL

5.3 Staff training

- As part of our E-safety yearly programme we will:
- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.

- The e-safety programme will have several ways identified per school where this will take place like; existing safeguarding and child protection training/updates or within separate or specific online safety sessions.
- This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as AE professional practice expectations.

- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the school, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.
- The E-safety officer will provide advice / guidance / training to individuals as required.

5.4 Parents and carers

- Aldridge Education recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
  - Providing information and guidance on online safety in a variety of formats.
    - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events and other opportunities.
  - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
  - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
  - Requiring them to read our acceptable use policies and discuss the implications with their children.

Trustees, governors, parents, carers, visitors, contractors and community users will also be included in our E-safety Programme with specific training and events for each group following e-safety best practice.

6. Monitoring, Incidents and Sanctions

- Technology in this area evolves and changes rapidly; Aldridge Education will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the CEO and principals will be informed of online safety concerns, as appropriate.
- Any concerns or incidents identified via monitoring will follow our safeguarding policy and procedures within each academy.
- The named governor for safeguarding in each academy will report on a regular basis to the local governing body on online safety practice and incidents, including outcomes as part of the safeguarding process and policy. Please refer to the Safeguarding policy for more information.

7. Links to Other Policies and Practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use policies
- Data Protection policy
- Safeguarding policy
- Social Media policy

8. Useful links on E-safety

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

9. Appendices

9.1. Virtual Learning Parental Consent Form

Virtual Learning Parental Consent Form

Virtual Learning: Student Agreement & Parental Consent

What is virtual learning?

During the school year, students may have the opportunity to join virtual learning classes or tutorials via our approved virtual learning technologies, Microsoft Teams or Google Meet. Interactive lessons enable students and teachers to collaborate through video, audio, screen and file sharing. These technologies are a great way to continue learning outside the traditional classroom environment.

We make sure that we have consider and planned appropriately for the smooth transition from classroom to blended learning and remote learning, so our staff have the knowledge and tools to provide a safe virtual learning environment to the students.

General information about our use of video conferencing and virtual learning technologies:

- All our approved platforms are fully end-to-end encrypted.
- The client software is generally available to be installed and used in most personal devices.
- The use of these virtual technologies will require access to the internet on student devices.
- Lessons are scheduled and prepared well in advanced by teachers.
- Staff and students must comply with all Aldridge Education policies while using these technologies the same way they will do as if they are in a normal classroom.
- We will make sure students understand the rules and expectations while using these technologies well in advance.

Consent points:

- I understand that as a parent or guardian, I am responsible for supervising the suitability of my child's/children's online access, communication, and the 'home' environment (wherever

distance learning is taking place outside of school). Ensuring students have a quiet, safe space from which to join these activities (in an appropriate room), are wearing appropriate clothing for learning, trying to maintain school uniform/dress, and that there are no age-inappropriate or background noises visuals or moving images. I understand that only my child(ren) will join the meeting, and that adults and other children will not be permitted to participate without prior agreement by all parties. Parents are encouraged to supervise in certain circumstances due to student age or other agreed reasons (but not appear on screen). Each meeting will end at the teacher's discretion.

- I understand that classroom teachers will approach virtual classrooms as being an extension of the school learning environment. As such, classroom expectations, procedures, policies, and rules will be adhered to as normal - by staff and students alike. Teachers will facilitate and lead all virtual classrooms and will follow Aldridge Education policies and classroom rules.
- Please refer to our e-safety policy for more detailed information about our safeguarding measures, practices, and security around these technologies.

☐ I give permission for my child(ren) to participate in virtual learning/video conferencing classes.
☐ I do not give permission for my child(ren) to participate in virtual learning/video conferencing classes.

Student Name: _____

Parent/Guardian Name: _____

Parent/Guardian signature: _____ Date: _____

Student Virtual Learning Agreement Form

Introduction

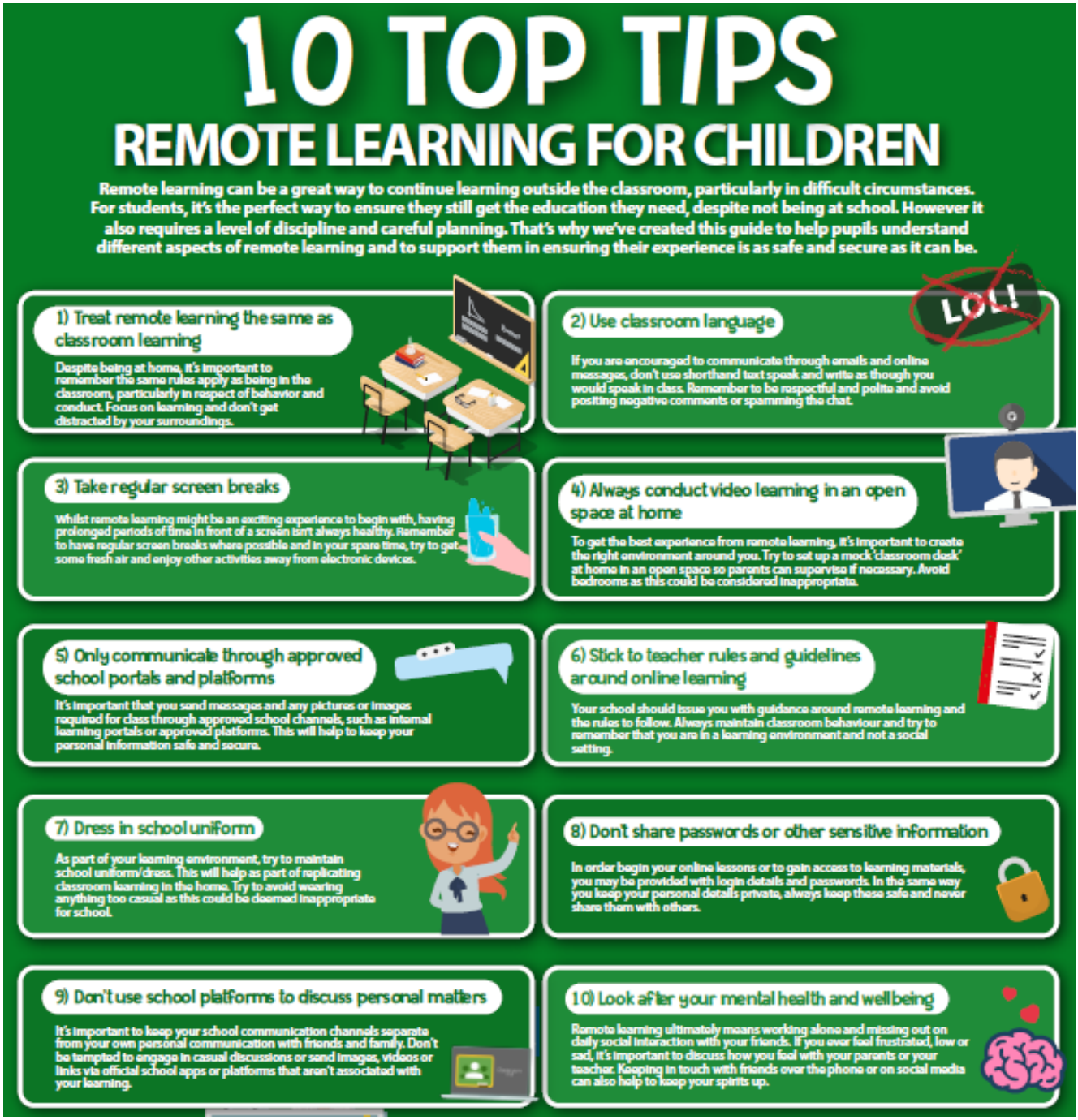
Below we explain some of the expectations that all students using the school virtual learning environment using Microsoft Teams or Google Meet will need to follow so that we can have a safe and fun virtual learning environment.

These are listed below, so can you read through them and let a teacher at school know if there's anything that you don't quite understand, or if you think any of the points might be difficult to follow. If so we will see-what we can do to help.

Once you have read through the points, please sign the form to show that you agree to follow them, and we will then send you the relevant Microsoft Teams or Google Meet invite; this will be done on a session by session basis.

Expectations:

- You need to be in your day clothes; the sort of thing you might wear on a non-uniform day, not pyjamas, low cut tops, vests, or similar
- You need to be in an area of your home where you will be comfortable and are less likely to be interrupted by members of your household
- You need to ensure that you have a laptop, tablet, or phone that you will be able to use for the duration of the session. If this may be a problem, then please let us know
- When taking part in the sessions, if your camera is enabled you will need to try and have a neutral background, preferably with no photos or personal items behind you
- Use the kind of language that would be expected of you when talking to staff at school or college – be respectful, considerate, and kind to everyone; staff, and other young people. Failure to do so could result in you being removed from the session and/or programme
- Do not share the session invite log-in details with anybody who is not part of the programme – choosing to do so can result in you being removed from the virtual classroom or programme
- Do not take, use, share, publish or distribute images of other young people on the programme without their permission; this includes taking screen shots
- You have read and understood the attached Remote learning for children poster



Student Name: _____

I agree to comply with the expectations outlined here.

Student Signature: _____ Date: _____