Alder Grove
Church of England Primary School

KEYS
Academy Trust

E-Safety Policy

Date	September 2020
Review Date	September 2021

The Keys Academy Trust

Data and E Safety Policy

Aim

The aim of this policy is to describe how the school will ensure the safety of pupils whilst using the internet and associated technologies. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2019, Early Years and Foundation Stage 2017 and 'Working Together to Safeguard Children' 2018.

Introduction

The Keys Academy Trust believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. The Keys Academy Trust identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. The Keys Academy Trust believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online. This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of our schools (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

The school's Data & E-Safety Policy will operate in conjunction with other policies including those for Behaviour, Disciplinary, Anti- Bullying, Curriculum and Data Protection.

Our Data & E-Safety Policy has been written by the Trust, following guidance from Wokingham Borough Council, Kent County Council and government guidance. It has been agreed by the senior leadership team and approved by the governors.

1. Roles and Responsibilities

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety. (Note: Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.) The Keys Academy Trust

recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

1.1 The Senior Leadership Team within our schools will:

- 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 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.

1.2 The Designated Safeguarding Lead within our schools will:

- 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 deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities.
- 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 and up to date knowledge 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, as appropriate, to the school's Senior Leadership Team.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (once per term) with the governor with a lead responsibility for safeguarding.

1.3 It is the responsibility of all members of staff in our schools to:

- Contribute to the development of online safety policies.
- Read and adhere to the E-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.
- 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.

1.4 It is the responsibility of staff managing the technical environment within our schools to:

- 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 security measures *(*e.g. enforced password protection, encryption of removable devices*)* as directed by the leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

- Ensure that the filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that the monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

1.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) in our schools to:

- 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.

1.6 It is the responsibility of parents and carers in our schools to:

- 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 home-school agreement 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 school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

1.7 It is the role of the Data Protection Officer to:

- Maintain registration with the Information Commissioner's Office
- Keep abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk

- Inform staff and SLT of these recommendations so that school policies may be updated. See Appendix 1 – School and the Data Protection Act for further information and the School Data Protection policy

2. Education and Engagement Approaches

2.1 Education and engagement with learners

- Our schools will establish 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), Computing programmes of study and a planned programme of assemblies.*
    - *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) and to respect copyright when using material accessed on the internet.*
    - *Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.*
- Our schools will support 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.*
    - *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 in accordance with our Behaviour Policy*
    - *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.*

2.2 Digital Literacy

- As part of the Computing Curriculum, our schools deliver discrete teaching of digital literacy and citizenship skills in supporting pupils to act responsibly and develop pupils' understanding of online safety.
- Our schools follow schemes of learning developed by South Western Grid for Learning for all year groups, from Foundation Stage to Year 6. These are based on

Common Sense Media's Digital Literacy and Citizenship Curriculum, which empowers learners to think critically, behave safely, and participate responsibly in our digital world. These 21st-century skills are essential for children and young people to harness the full potential of technology for learning.

2.3 Vulnerable Learners

- The Keys Academy Trust 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.
- Our schools will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate E-Safety Policy and curriculum our schools will seek input from specialist staff as appropriate, including the SENCO and Child in Care Designated Teacher.

2.4 Training and engagement with staff

Our schools will:

- Provide and discuss the E-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 as part of existing safeguarding and child protection training.
    - This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our 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 setting, 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.

2.5 Awareness and engagement with parents and carers

- The Keys Academy Trust 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.
- Our schools 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, fetes and sports days.
    - Drawing their attention to the E-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.
    - Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is available to parents via the Online Safety link on our learning platform.

3. Reducing Online Risks

- Our schools recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- They 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.

4. Safer Use of Technology – see appendix A for school specific data

5. Social Media

5.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members in all of our school 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 messengers.
- All members of our community within our schools are expected to engage in social media in a positive, safe and responsible manner.
    - All members of our communities within our schools 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.
- The schools will control learner and staff access to social media whilst using setting provided devices and systems on site. (***Settings should detail further information regarding access according to their approach***)
    - The use of social media during school hours for personal use is not permitted.
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member within our school communities on social media, should be reported to the DSL within the specific school and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

5.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of any of the schools within The Keys Academy Trust on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy) and/or the Head of School.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

5.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.

- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

5.4 Official Use of Social Media

- Alder Grove CofE Primary School official social media channels are:
  Twitter: @aldergrove3
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the *Head of School*.
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected and, where possible, run *and/or* linked *to/from* our website.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role *and/or* position but make it clear that they do not necessarily speak on behalf of the setting.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure that they have appropriate consent before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
    - Inform their line manager, the DSL (or deputy) and/or the *Head of School/manager* of any concerns, such as criticism, inappropriate content or contact from learners.

Appendix 1 – Exemplar Acceptable Use Agreements

The following are included as possible starting points in developing appropriate agreements and guidelines for individual schools. It is highly unlikely that they will be suitable without amendment and are also likely to require consultation with the respective stakeholders.

The exemplars included are:

- Student/Pupil Acceptable Use Agreement
- Parent/Carer Acceptable Use Agreement
- Exemplar Laptop Acceptable Use Agreement
- Staff Acceptable Use Agreement

Appendix A – Classroom use

Alder Grove CofE Primary School

4.1 Classroom Use

- Our school uses a wide range of technology. This includes access to:
    - *Computers, laptops, tablets and other digital devices*
    - *Internet which may include search engines and educational websites*
    - *Digital cameras, web cams and video cameras*
- All school owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
    - Tablets are managed through a Device Management software and access is monitored through NetSupport
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. The school advises that the following search engines are used:
    - *SWGfL Squiggle*
    - *Dorling Kindersley find out*
    - *Google Safe Search*
    - *School created Google custom searches*
    - *CBBC safe search*.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law 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 learners age and ability.

4.2 Managing Internet Access

- Alder Grove CofE Primary School will maintain a written 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

4.3.1 Decision Making

- Alder Grove CofE Primary School school governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders 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 by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team 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.

4.3.2 Filtering

- Education broadband connectivity is provided through TalkTalk for Alder Grove Primary School.
- We use RM Safety Net which blocks sites which can be categorised as: pornography, racial hatred, extremism, social networking, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with RM Safety Net to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Turn off the monitor or minimise the window immediately
    - If monitor cannot be turned off quickly, the device can be placed screen down.
    - Report the incident to the teacher or responsible adult.
    - Our teachers should
        - Ensure the well-being of the pupil.

        - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
        - Report the details of the incident to the DSL (or deputy) and/or technical staff.
        - Log incident on CPOMS.
    - The DSL will then
        - Review the incident and take any appropriate action.
        - Inform parents/carers 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.

4.3.4 Monitoring

- Alder Grove CofE Primary School will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - Physical monitoring (supervision)
    - Monitoring internet and web access (reviewing logfile information)
    - Active technology monitoring services provided by NetSupport
- If a concern is identified via monitoring approaches we will:
    - DSL or deputy will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

4.3.5 Complaints Regarding Internet Use

- Our school has procedures in place for dealing with any complaint of Internet misuse.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Complaints of Internet misuse will be dealt with by the Head of School.
- Any complaint about staff misuse will be referred to the Head of School.

4.3.6 Sanctions

- Our schools have a system of sanctions to promote the appropriate use of technology.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter as far as staff are concerned.

4.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our information security policy.

4.5 Security and Management of Information Systems

- Alder Grove CofE Primary School will take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for 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 held on our network,
    - The appropriate use of user logins and passwords to access our network.
        - Specific user logins and passwords will be enforced for all but children in EYFS.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be found under our acceptable use policies.

4.5.1 Password policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

- All passwords used by adults should follow the guidelines in this policy.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a child.
- No individual should tell another individual their password.
- Once a computer has been used, users must remember to log off so that others cannot access their information. Users leaving a computer temporarily should lock the screen.

- Passwords must be changed every half term and must meet complexity requirements. A security setting determines whether passwords meet these requirements. These requirements are enforced when passwords are changed or created. The minimum requirements are that a password must:
    - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
    - Be at least six characters in length
    - Contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphabetic characters (for example, !, $, #, %)
- Passwords must not be easily guessable by anyone.
- If a password is identified as insecure then it is essential that the password is changed immediately.

4.6 Managing the Safety of our Website

- Alder Grove CofE Primary School will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- They will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- Our schools will post appropriate information about safeguarding, including online safety, on our website for members of the community.

4.7 Publishing Images and Videos Online

- Alder Grove CofE Primary School will ensure that all images and videos shared online are used in accordance with the associated polices, including the: data security policy, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

4.8 Managing Email

- Access to our schools' 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 permitted.
    - 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.
    - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the DSL (or deputy) 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 (e.g. GoogleMail) may be blocked on site.

4.8.1 Staff email

- The use of personal email addresses by staff in our schools for any official school business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- All of our 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.

4.9 Management of Applications (apps) used to Record Children's Progress

- Alder Grove CofE Primary School uses Target Tracker to track learners progress and share appropriate information with parents and carers.
- The Head of School is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - Only school issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.

- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Student/Pupil Acceptable Use Agreement

This agreement will need amending to suit the age of the students/pupils concerned.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems and other digital communications.
- I will not tell anyone my username or password nor will I try to use any other person's username and password.
- I will be aware of 'stranger danger', when I am communicating online.
- I will not give out any personal information (e.g. home address and telephone number) about myself or anyone else when online.
- I will not arrange to meet people offline that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

Acting as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

Keeping secure and safe when using technology in school:

- I will only use my personal handheld/external devices (e.g. mobile phones, USB devices, etc.) in school if I have permission and I understand that if I do use my own devices in school I must follow the rules as if I was using school equipment.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will immediately tell a staff member if I receive an offensive e-mail or message.

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (e.g. cyberbullying, inappropriate use of images and/or personal information).
- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

I have read and understood the above and agree to follow the rules outlined.

Name:	
Signature:	
Date:	

Parent/Carer Acceptable Use Agreement

The school seeks to ensure that *students/pupils* have good access to ICT to enhance their learning and, in return, expects *students/pupils* to agree to be responsible users. A copy of the *Student/Pupil* Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

==========

Acceptance of Use Form

Parent/Carer's Name:	
Student/Pupil's Name:	

As the parent/carer of the above *student/pupil*, I understand that my son/daughter will have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

Signature:	
Date:	

Staff Laptop/Devices Acceptable Use Agreement

1. Introduction

- This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
- It should be read in conjunction with the school's E-Safety Policy
- All recipients and users of these devices should read and sign the agreement.

2. Security of equipment and data

- The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
- Staff should understand the limitations of the school's insurance cover so therefore laptops/devices should not be left in vehicles at any point.
- Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

3. Software

- Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
- Only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
- Users should not attempt to make changes to the software and settings that might adversely affect its use.

4. Faults

- In the event of a problem with the computer, the school's ICT Technician/Network Manager should be contacted.

Declaration:

I have read and understood the above and also the school's E-Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	

Staff Acceptable Use Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-Safety Policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Head of School.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school E-Safety Policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that pupil use of the internet is consistent with the school's E-Safety Policy.
- When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. Online Safety Co-ordinator and/or SLT member.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:	
Signature:	
Date:	

Social Networking Acceptable Use Policy for Staff

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety. I am aware that Facebook and Twitter are public and global communication tools and that any content posted may reflect on the school, its reputation and services.
2. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.
3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead and/or the Head of School. The Head of School retains the right to remove or approve content posted on behalf of the school.
4. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
5. I will follow the school's policy regarding confidentiality and data protection/use of images.
    - This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community.
    - Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school via school owned devices. Images taken for the sole purpose of inclusion on (tool using) will not be forwarded to any other person or organisation.
6. I will promote online safety in the use of Facebook and Twitter and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by the Designated Safeguarding Lead/Head of School prior to use.
7. I will set up a specific account/profile using a school provided email address to administrate the accounts on Facebook and Twitter and I will use a strong password to secure the account. Personal social networking accounts or email addresses will not be used.
    - The school Designated Safeguarding Lead and/or Head of School will have full admin rights to the (tool using) site/page/group.
8. Where it believes unauthorised and/or inappropriate use of Facebook and/or Twitter or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
9. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.
10. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Head of School and/or Designated Safeguarding Lead urgently.
11. I will ensure that the (tool using) site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.
12. I have read and understood the school E Safety Policy which covers the requirements for safe IT use, including using appropriate devices and the use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the Head of School.

13. If I have any queries or questions regarding safe and acceptable practice online, I will raise them with the Designated Safeguarding Lead (name) or the Head of School.

I have read, understood and agree to comply with the Social Networking Acceptable Use Policy for Staff.

Signed: …….. Print Name: …… Date: ……
Accepted by: ……. Print Name: …….