



ALMOND HILL JUNIOR SCHOOL
GOVERNING BODY

Online safety including remote
learning, mobile phone use and
social media

Full Governing Body	September 2023
Date for Review	September 2024

Contents

1.	Introduction	3
	Process for monitoring the impact of the Online Safety Policy.....	3
2.	Scope of policy	3
3.	Responsibilities	4
	Headteacher and Senior Leaders	4
	Governors	4
	Designated Safety Lead (DSL)	5
	Online Safety Lead.....	5
	Online Safety Group.....	6
	Curriculum Leads	6
	Teaching and support staff	6
	IT Provider	7
	Learners	7
	Parents and carers.....	7
4.	Policy and procedure.....	8
	Use of email.....	8
	Visiting online sites and downloading.....	8
	Digital and Video Images.....	9
	Use of personal mobile devices (including phones)	10
	The use of social media for staff.....	10
	Prohibited use.....	11
	Business use of social media	11
	Guidelines for the responsible use of social media	11
	Online Publishing	11
	Filtering and Monitoring	12
	Breach of this policy	12
	New technological devices	12
	Reporting incidents, abuse and inappropriate material	13
	Data Protection.....	13
5.	Curriculum	13
6.	Staff and Governor Training	14
7.	Working in Partnership with Parents/Carers.....	14
8.	Records, monitoring and review	14
	Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff).....	15
	Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers	18
	Appendix C - Requirements for visitors, volunteers and parent/carers helpers	21
	Appendix D - Online Safety Acceptable Use Agreement Primary Pupils.....	22
	Appendix F - Guidance on the process for responding to cyberbullying incidents.....	25
	Appendix G - Guidance for staff on preventing and responding to negative comments on social media.....	26
	Safeguarding and remote education during coronavirus (COVID-19)	Error! Bookmark not defined.
	Useful resources	Error! Bookmark not defined.

1. Introduction

Almond Hill Junior School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- filtering and monitoring logs
- surveys/questionnaires of:
 - learners
 - parents and carers
 - staff

2. Scope of policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels – stored on the Cloud and staff alerted via email of any changes
- *is published on the school website.*

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: Keeping Children Safe in Education, Data Protection Policy and Breach Response Plan, Health and Safety, Behaviour, Anti-Bullying and PSHE/RSE policies.

3. Responsibilities

This Online Safety Policy has been developed by:

- Headteacher/senior leaders
- Designated safeguarding lead (DSL)
- Online Safety Lead (OSL)
- Governors
- The School Business Manager

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is **Roisin Lyons**.

All breaches of this policy that may have put a child at risk must also be reported to the **Headteacher who is the DSL**.

Organisations that are renting space from the school and are a totally separate organisation, should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, Cloud-based services and/or equipment, then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

Headteacher and Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, The day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the designated safeguarding lead (DSLs) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the

policy.

The review will be carried out by The Governing Body whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the [DfE Filtering and Monitoring Standards](#)
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the [DfE Cyber-Security Standards](#)

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

At Almond Hill, the DSL is **Emma Fordham** (headteacher) with **Shahnaz Birchall and Gemma Burgess as deputies.**

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities.

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- report regularly to the Full Governing Body to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

At Almond Hill, the Online Safety Lead is **Roisin Lyons.**

The Online Safety Lead will:

- lead the Online Safety Group
- work closely with the Designated Safeguarding Lead (DSL),
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with pastoral staff and support staff
- receive regularly updated training to allow them to understand how digital technologies are used and are

developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:

- o content
- o contact
- o conduct
- o commerce

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives.

The Online Safety Group has the following members:

- Online Safety Lead
- online safety governor
- technical staff
- teacher and support staff members
- learners
- parents/carers

Members of the Online Safety Group (or other designated group) will assist the DSL/OSL with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement
- they immediately report any suspected misuse or problem to the DSL or deputies for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a

- good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the [DfE Meeting Digital and Technology Standards in Schools & Colleges](#)
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy including personal devices where allowed
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the Data Protection Policy and Breach Response Plan. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Headteacher/School Business Manager.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer (Richard Maskrey, contactable via SBM) with details of the site/service and seek approval from SBM. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites may be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.
- When working with pupils, searches should be done through the Securely Filter (or a similar application) that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

The school has moved to The Cloud. Staff using The Cloud have been instructed to ensure any downloads are removed and no copies are left on their device. Downloads will automatically be deleted if they have not been opened in 30 days.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, recorded, and permission given by the Headteacher.

Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes. Records are kept on Arbor and consent can be changed by parents/carers at any time. (See Data Protection Policy and Breach Response Plan for greater clarification).
- staff/volunteers must be aware of those learners whose images must not be taken/published. Images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images. Parents are reminded of this.
- Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's

Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- Photographs and videos/media of pupils are only stored on the school's agreed secure networks which include some Cloud based services.
- Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of parents/carers.
- Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.
- Rights of access to stored images are restricted to approved staff as determined by the Headteacher.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device without withholding their number and this would always be if there was no viable alternative.

We prefer parents not to use their phones on school premises.

Entering the school, visitors are made aware of our mobile phone procedure. They are asked to turn their phones to silent and not to use them in teaching areas of the school.

Pupils in year 5 and 6 are allowed to bring personal mobile devices/phones to school if they come to school independently but must switch off as they enter school and not use during the school day. Phones will be kept in a box in classrooms and collected by pupils at the end of the school day. The school does not allow pupils to carry mobile phones on trips or visits including residential visits. Parents will be reminded of this when they receive information about any trips/visits. The school takes no responsibility for phones at school. Under no circumstances should pupils use their mobile phones to take pictures whilst on school premises. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles can only be used to access school e-mail and data where there are 2 layers of security. This means there is a password to access the device and a further password to access the e-mail/data. Therefore, e-mail apps cannot be used if this means they remain open.

Children are not permitted to wear 'smart' watches in school.

The use of social media for staff

Social media has been defined as any online platform that allows parties to communicate with each other or share data in a public forum.

Employees must limit their personal use of social media on their own equipment to rest breaks such as lunch or breaktimes.

Prohibited use

Employees must not abuse their position of trust with pupils including, but not limited to:

- Accepting any current pupils or former pupil under the age of 18 as friends, or requesting such friendships
- Communicating personally with pupils
- Posting photographs of pupils on sites not agreed by the school
- Commenting about or naming pupils

Employees must avoid making any social media communications that could damage the school's interests or reputation even indirectly.

Employees must not use social media to:

- Defame or disparage the school, its employees or any third party
- Harass, bully to unlawfully discriminate against staff or any third parties
- Make false or misleading statements
- Impersonate colleagues or third parties

Business use of social media

If an employee is contacted for comments about the school for publication anywhere including social media, the enquiry should be directed to the Headteacher and the employee should not respond without their written approval.

The employee must not express opinions on the school's behalf unless authorised to do so by the Headteacher. The employee should not post comments about sensitive school-related topics, such as the school's performance, internal disputes involving pupils, parents or employees or do anything to jeopardise the school's confidential information regarding pupils and other employees. They must not use the school's logo or any other trademarks unless expressly authorised to do so.

Employees should never provide professional references on behalf of the school for other individuals without the express authority of the Headteacher including those on social networking sites. These whether positive or negative can be attributed to the school and create legal liability for the author and school.

Guidelines for the responsible use of social media

The employee should make it clear in social media postings that they are speaking on their own behalf. They should be respectful to others when making any statement on social media and be aware they are personally responsible for all communications which are published on the internet for anyone to see. Employees should use the privacy and access settings whilst being aware that they cannot control the use of their postings by others.

If the employee becomes aware of social media content that disparages or reflects poorly upon the school, they should contact the head teacher.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- *Other (e.g., Facebook)*

The school website is managed/hosted by E4Education. The school ensures that online safety policy has been

followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

Filtering and Monitoring

The school reserves the right to monitor, intercept and review, without any further notice, employee activities using school, IT resources and communication systems, including but not limited to social media postings and activities to ensure that school rules are being complied with and for legitimate school purposes.

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor.

- the school manages access to content across its systems for all users and on all devices using the school's internet provision.
- *the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for and different groups of users: staff/learners, etc.)*
- *twice a week the onsite engineer checks filtering is effective. Once checked, this is confirmed by email to the Headteacher and School Business Manager*

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services using 'Securely' whereby the SBM and headteacher receive pro-active notifications for any breaches allowing effective intervention
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

Breach of this policy

Breach of this policy may result in disciplinary action up to and including dismissal. The employee may be required to remove any social media content that the school considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and discuss and minute before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the Headteacher before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL, the Headteacher or School Business Manager. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy and Breach Response Plan.
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it

5. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum and Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity.
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment.
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives). Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online.
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others.
- Understanding the permanency of all online postings and conversations.
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse.

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school checks the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix C).

7. Working in Partnership with Parents/Carers

Parents/carers are asked on admission to read, discuss with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix E. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Online safety incidents involving pupils are recorded on the school CPOMs system.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)

You must read this agreement in conjunction with the online safety policy and the Data Protection Policy and Breach Response Plan. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Head teacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will only use the school's email/intranet/internet and any related technologies for professional purposes or for uses deemed reasonable by the Chair of Governors.

I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Headteacher/School Business Manager

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

I will not initiate any communication with pupils using mobile phone technology within 5 years of leaving the school unless there is a parental link.

When using video calls to communicate with children, parents or visitors I will ensure my background is appropriate and that the camera is positioned to only provide a headshot.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member. All visitors to the school must use the visitor account supplied by the school business manager.

Data protection

I will follow requirements for data protection as outlined in Data Protection Policy and Data Breach Response Plan. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the Head Teacher or governing body
- Personal or sensitive data taken off site must be encrypted
- I will respect copyright and intellectual property rights.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

When downloading files onto a personal device, I will ensure all downloads are removed from the device and stored on the Cloud.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Headteacher.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL or deputy DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Headteacher.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSL. A school-owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature Date

Full Name (printed)

Job title

Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers

School name Almond Hill Junior School

Online safety lead Mrs R Lyons

Designated Safeguarding Lead (DSL) Headteacher

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Headteacher/School Business Manager

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

I will not share my professional details, such as mobile phone number or email address, with parent/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I

understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member. Visitors must log in using the visitor password via the School Business Manager.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the headteacher/DSP, or a young person's or parent/carer's own device.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Headteacher.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL or Deputy DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Headteacher.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation’s contract with the school.

Signature Date

Full Name (Please use block capitals)

Job Title/Role

Appendix C - Requirements for visitors, volunteers and parent/carers helpers

(Working directly with children or otherwise)

School name Almond Hill Junior

Online safety lead Mrs R Lyons

DSL: Head teacher

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSL

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSL or headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared on line, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Appendix D - Online Safety Acceptable Use Agreement Primary Pupils

My online safety rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Appendix E – Acceptable use agreement for pupils and parents

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding of this policy and agreements
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, we prefer phone/s to be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Remote Learning (In the event of need)

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you).

The school will:

- Provide a continuous connection with your child via Microsoft 'Teams' to offer them routine and support
- Continue to nurture your child through contact to ensure they are happy, safe and well during these unsettling times
- Provide remote learning tasks with explanation and instruction
- Respond to any concerns you may have in a timely manner within school hours.

As a pupil of Almond Hill, I will

- Engage in my daily learning tasks and respond to my teacher appropriately through Teams or in phone call conversation so they know I am happy, safe and I am engaging in my learning.
- I understand my behaviour in remote learning responses should mirror that in the physical classroom

Possible sanction for failing to comply with this agreement will be removal of access to Microsoft Teams for your child/children

As a parent/carer I will

- Encourage your child to engage with their daily learning tasks.
- Ensure any queries you have are directed to the class teacher via the year group email within school hours
- Offer understanding and support to teachers who may encounter technical difficulties
- Not use social media to make negative commentary of the school

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

A signature is not required for this document, the terms herein are confirmed by all parties upon receipt.

Appendix F - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix G - Guidance for staff on preventing and responding to negative comments on social media

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

REMOTE LEARNING (IN THE EVENT OF NEED)

Aims:

- Pupils have equal access to devices to enable to them fully participate in the activities involved in remote learning.
- Pupils can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- Pupils are responsible, competent, confident and creative users of information and communication technology.
- Pupils can continue their **education remotely, using Microsoft Teams as a teaching and learning platform.**

CURRICULUM ORGANISATION

Throughout KS2, computing is embedded across the curriculum. A range of digital technologies and software are used to support subjects across all areas of the curriculum. Microsoft Teams is used as a platform for children learning remotely either during a period of time when school is not open to all pupils. Remote teaching involves each class receiving weekly home learning assignments and to give instructions for the work that day and explaining anything that is required, allowing children to respond and 'hand in' responses to class teachers.

Remote learning assignments will be posted and responded to by class teachers.

TEACHING AND LEARNING STRATEGIES

The use of technology throughout the curriculum enables children to develop skills that are vital for success in later life, such as:

- collaboration
- communication
- problem-solving
- resilience
- perseverance
- team-work

In studying computing, pupils experience a variety of approaches to their learning including:

- Teacher demonstrations
- Individual and shared use of digital devices
- Collaborative work
- Open-ended investigation

In remote learning, staff are able to set assignments for children that they can respond to. Teachers can comment on their responses.

When teaching remotely, teachers will:

- Provide frequent, clear explanations of new content, delivered by a teacher in the school or PowerPoints with voice over.

RECORD KEEPING AND ASSESSMENT

Assessment is a central part of the learning process. Assessment can be carried out by:

- reviewing 'handed in' returned outcomes
- speaking to pupils in Teams meetings
- speaking to pupils on the phone

STAFF DEVELOPMENT

It is important to provide training for all staff to enable them to deliver the computing curriculum to their pupils. School based INSET training needs to be given to enable teachers to familiarise themselves with software and technology relevant to the school. All staff will be given training via the Computing Lead.

Before working remotely, staff underwent training on how this would work in practice and how to safeguard themselves while working from home.

INTERNET AND E-MAIL

Staff should refer to the Code of Conduct and remind pupils of the Code of Conduct at the beginning of any lesson using these resources. This should be included as a lesson objective.

PREVENT AGENDA

The Prevent duty guidance says 'having due regard' requires schools and colleges to:

- (a) have "robust safeguarding policies in place to identify children at risk and intervening as appropriate;"
- (b) provide staff with training "that gives them the knowledge and confidence to identify children at risk of being drawn into terrorism and to challenge extremist ideas"; and
- (c) (c) "ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering".

- Prevent Duty Guidance - July 2015 (England and Wales) <https://www.gov.uk/government/publications/prevent-duty-guidance>

[Staff should be mindful to this duty when monitoring pupil engagement in all areas of computing including remote learning.](#)

HEALTH AND SAFETY

Children will be reminded of good practice for use of technology for remote learning e.g. screen time and taking regular breaks.

CHILD PROTECTION

All staff should be aware of the school policy on Online Safety, whether working in school or remotely, which sets out our expectations relating to:

- Creating a safer online environment
- Giving everyone the skills, knowledge and understanding to help children and young people stay safe online, question the information they are accessing and support the development of critical thinking
- Inspiring safe and responsible use and behaviour
- What steps to take if you have concerns and where to go for help

All children and staff will have access to Microsoft Teams as part of their remote learning. When video calling through Teams, children and staff should have a neutral background. Staff should ensure that their camera is positioned in a way that only a headshot of them can be seen. Where possible, children should have an adult at home who is aware that they are using Teams and are monitoring that they are using it appropriately.

It may be necessary for staff to record meetings with parents to ensure clarity of conversation from the safeguarding perspective of both staff and children. Parents/carers will be informed in a meeting is being recorded and agree to this verbally.

When uploading work, children, parents and staff should ensure that the content is appropriate to share within the school network.

COPYRIGHT

Unauthorised copying of software is illegal. Breach of copyright is theft. The prevention of unauthorised copying is the responsibility of the teacher, the Headteacher and the Governors.



ALMOND HILL JUNIOR SCHOOL REMOTE TEACHING GUIDANCE

In the event of your child not being able to attend school we will implement remote teaching via Microsoft Teams.

What can you expect to see as part of your child's remote education?

- All children will have been taught how to log on to their Teams account and will have been using this for home learning.

In the event of self-isolation (the rest of the year group are in school).

- Each week (from the second day of absence), children will be assigned tasks for English, Maths and Foundation subjects.
- There will be a PowerPoint to provide explanations and instructions for the tasks .
- Tasks will be set that continue to follow the curriculum of the year group and will cover a broad range of subjects.
- During the period of the isolation, pupils should return work to the teacher via 'Teams' and if that is not possible, complete work on paper and return this to school when coming back.
- During the period of self-isolation, parents can expect that teachers will contact children if the self-isolation is a week (5 days or longer). The teacher will send a parent an e mail to set up a 'Teams' meeting or will make a phone call home.

In the event of 'bubble' closure or whole school lockdown.

- Children will take home an exercise book in order to record their work if needed/possible.
- Each day children will be assigned tasks for English, Maths and Foundation subjects including PE.
- There will be a PowerPoint with teacher voice over to provide explanations and instructions for the tasks.
- Tasks will be set that continue to follow the curriculum of the year group and will cover a broad range of subjects. The time allocated will be of equivalent length to the core teaching in school. The school will signpost extension and additional activities for pupils to access. Tasks will be differentiated and children with SEND who have Individual Education Plans, will have specific tasks and access to the SENCO for support via the SENCO e mail, phone call or 'Teams' meeting.
- During the period of the shutdown, teachers will expect children to '*hand in*' completed assignments using 'Teams'. Where this is not possible, children will have recorded their learning task in their exercise book.
- For those pupils who do not have access to technology, the school will provide work packs to be collected. If any parent has difficulty in collecting a pack they should contact the school office to make alternative arrangements.
- Teachers will respond to '*handed in*' tasks; they will type a response. It will be possible to contact teachers via the year group e mail.
- During a week of shutdown, there will be 2 assemblies for children to view.
- It is expected that in returning assignments children will follow the school's Code of Conduct for remote learning . Any general comments that a pupil types in can be viewed by teacher and other pupil and these will be monitored by class teacher. Children will be aware of the Code of Conduct for Remote Learning and parents will be contacted immediately if their child does not adhere to our expectations.
- As with any use of technology, parents should monitor their child's use and there should be a balance of on screen and off screen time in the day.