Alsager Highfields Primary School

Mighty oaks from small acorns grow

Nurture, Believe, Achieve

Online Safety Policy

Written in conjunction with our Child Protection and Safeguarding policy, Behaviour policy, Mobile Phone, Digital Device and Social Media Policy, Staff Code of Conduct handbook and guidance for safer working practice.

Prepared by Mrs M Dyde

September 2024

Chair of Governing Board: Mr Alan Stancliffe

Signature: Alan V. Stancliffe.

Date: Sept. 2024.

Date to be reviewed: to be reviewed in light of operating experience, changes to personnel or changes to legislation.

The Cornovii Trust

Online Safety Policy

Introduction

Alsager Highfields Primary School is pleased to offer pupils access to a computer network for the internet and a wide range of computing resources. To gain access to the internet, all pupils must obtain parental/carers' permission. Should a parent prefer that a student does not have Internet access, use of the computers is still possible for other work such as word processing and coding. Codes of conduct and permissions are found in the children's reading diaries.

Access to the internet carries with it the danger that children could find and view material that is unsuitable for them or that they could be put at risk from unwanted and inappropriate contacts. This policy seeks to ensure that the internet is used appropriately for learning but with safeguards to protect children from harm. This policy will operate in conjunction with other important policies in our school, including our Mobile Phone, Digital Device and Social Media Policy, Behaviour, Antibullying and Child-on-Child Abuse Prevention Policy, Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR), Child Protection and Safeguarding Policy, Computing Policy, Education for a Connected World, Teaching online safety in school, Sharing nudes and semi-nudes: advice for education settings working with children and young people, Harmful online challenges and online hoaxes, Health and Safety Policy, Equality and Diversity Policy, Complaints Policy and Statutory guidance for schools and colleges - 'Keeping children safe in education' DfE September 2024.

Aims

Alsager Highfields Primary School believes that every child should have the right to a curriculum that champions excellence; supporting pupils in achieving the very best of their abilities. We understand the immense value technology plays not only in supporting the Computing and whole school curriculum but overall in the day-to-day life of our school. We believe that technology can provide: enhanced collaborative learning opportunities; better engagement of pupils; easier access to rich content; support conceptual understanding of new concepts and can support the needs of all our pupils.

Our aims:

- To provide an exciting, rich, relevant and challenging computing curriculum for all children.
- To enthuse and equip children with the capability to use technology throughout their lives. To give children access to a variety of high-quality hardware, software and unplugged resources.
- To instil critical thinking, reflective learning and a 'can do' attitude for all our pupils, particularly when engaging with technology and its associated resources.
- To teach pupils to become responsible, respectful and competent users of data, information and communication technology.
- To use technology imaginatively and creatively to inspire and engage all pupils, as well as using it to be more efficient in the tasks associated with running an effective school.
- To equip pupils with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimise risk to themselves or others.

- To ensure that children's access to inappropriate sites and locations is restricted.
- To ensure that the use of the internet is for proper purposes related to the teaching, learning and curriculum of this school.
- To protect children from harm and upset that could be caused through access to inappropriate sites, materials, images and contacts.
- To make children aware that there are inappropriate sites that are harmful and which must be avoided in school and at home.
- To encourage children to report immediately any inappropriate sites, materials or contacts that they find on the internet, either at school or at home.
- To raise awareness with older children in school, who are likely to be using computers independently at home of the potential risks and dangers of internet use.
- To ensure GDPR compliance is met and fully adhered to. Any breaches are recorded on the school's software system (GDPRiS).

Online Safety

Online safety has a high profile at Alsager Highfields Community Primary School for all stakeholders. We ensure this profile is maintained and that pupil needs are met by the following:

- A relevant up-to-date online safety curriculum which is progressive from Early Years to the end of Year 6.
- A curriculum that is threaded throughout other curriculums and embedded in the day-today lives of our pupils.
- Training for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- Through our home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.

- Appropriate firewalls are in place and must be enabled at all times on all the school computers. Anti-virus software is also installed and kept up-to-date. The school filter and monitoring system (Schools Broadband) produces reports which go to the Headteacher / Assistant Headteacher who then informs the relevant person about it. It is a robust and appropriate monitoring and filtering system. "Over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.
- Staff must not under any circumstances, or at any time, disable- or bypass firewalls on any school-owned computer.
- SECURUS is installed on every computer and laptop. This highly secure, easy-to-use, cloud-based server console captures words and phrases – and stores associated screenshots – enabling the DSL or safeguarding team to easily access dashboard reports to review and manage captures that are of concern or include inappropriate content.

- Children will be supervised by adults when they are given access to the internet.
- Children have their own log-ins for their computers.
- Parents/Carers have to sign an 'Equipment Loan Agreement' document which outlines acceptable use of their own computer when inside and outside of school. If this agreement is broken, school will ask for the device to come back into school.

- Staff must only use computers for school purposes. School computers used by staff at home or in school must not be modified or used for personal use.
- Staff using laptops in their classroom, or when logging on around school ensure that the screens are locked when not being used, or in the room by pressing the appropriate keys
- Children must be encouraged to notify staff if they, at any time, come across unsuitable material on a computer or a tablet.
- School staff must notify the Headteacher immediately if they find unsuitable or inappropriate material on a computer or storage device.
- Spot checks and audits will be carried out from time-to-time to ensure that computers are being used appropriately.

E-safety lessons are taught regularly throughout the school using a range of resources including Think U Know assemblies, celebrating and highlighting awareness on Safer Internet Day each year in February and our computing curriculum, Teach Computing Children are taught to:

- ✓ Take responsibility for keeping themselves and others safe online.
- ✓ Keep their usernames and passwords safe.
- ✓ Look out for cyberbullying and what to do if it occurs.
- ✓ Understand the importance of playing games which are age appropriate.
- ✓ Consider their digital footprints.
- ✓ Recognise when a news story might be fake.
- ✓ Assess their time spent online.

The lessons are all linked to the document: Education for a Connected World from the UK Council for Child Internet Safety.

- ➢ School will disseminate advice regarding E-Safety issues for parents/carers via the school website, text message service and newsletter.
- ➢ School governors should be aware of how E-Safety is taught at school and to robustly evaluate policies and procedures relating to this subject. Regular updates in governor meetings are very important with any breaches of the policy referred to.

INCLUSION

At Alsager Highfields Primary School, we aim to enable all children to achieve their full potential. This includes children of all abilities, social and cultural backgrounds, those with disabilities, children with EAL and children with SEND.

We place particular emphasis on the flexibility technology brings to allowing pupils to access learning opportunities, particularly pupils with SEND.

Monitoring, Evaluation and Feedback

Monitoring standards of teaching and learning within Computing is the primary responsibility of the Computing Lead. All teachers are expected to keep an online portfolio or track children's work. This portfolio must contain work samples from areas of the curriculum taught for the year group. Details of monitoring and evaluation schedules can be found in the Computing Action Plan and School Monitoring Schedule.

Roles and Responsibilities

Due to technology extending beyond the National Curriculum for Computing, there are key roles and responsibilities specific members of staff have.

Head Teacher

- Monitoring the implementation of the Computing Policy and its associated policies such as the Safeguarding and SEND Policies.
- Ratifying (in conjunction with the Governing Body) the Computing policy, Safeguarding policy and Computing Leader's Action Plan.
- Securing technical support service contracts and infrastructure maintenance contracts.
- Approving CPD and training which is in line with the whole school's strategic plan.
- Approving budget bids and setting them.
- Creating in conjunction with the Computing Leader, a long-term vision for Computing which includes forecasted expenditure and resources.
- Monitoring the performance of the Computing Leader in respect to their specific job role description for Computing.
- Ensuring any government legislation is being met.

Computing Lead

- Raising the profile of Computing for all stakeholders.
- Monitoring the standards of Computing and feeding back to staff in a timely fashion so
- they can act on areas for development.
- Ensuring assessment systems are in place for Computing.
- Maintaining overall consistency in standards of Computing across the school.
- Reporting on Computing at specific times of the year to the Governing Body/Head/Staff.
- Auditing the needs of the staff in terms of training/CPD.
- Actively supporting staff with their day-to-day practice.
- Seeking out opportunities to inspire staff in developing their practice through modelling
- and sharing new ideas, approaches and initiatives.
- Attending training and keeping abreast with the latest educational technology initiatives.
- Using nationally recognised standards to benchmark Computing.
- Creating Action Plans for Computing and supporting a long-term vision which feeds into
- the whole school development plan.
- Keeping an up-to-date log of all resources available to staff.
- Procuring physical and online resources that demonstrate best value.
- Reviewing the Computing curriculum and developing it as needed.
- Working as needed with the SENCO/Head Teacher to ensure online safety provision is above adequate and all legislation is in place.

Apex Technical Support

- Conducts routine scheduled maintenance/updates on systems.
- Supports the administration and set-up of online services including the school website.
- Fixes errors/issues with hardware and software set-up, prioritising as needed.
- Routinely checks school filtering, monitoring and virus protection.
- Sets up new hardware and installations.
- Maintains network connectivity and stability.
- Supports the Computing Leader and Head Teacher with future infrastructure needs and associated projected costs.

Cyber Security

Cyber security is about protecting the devices we all use and the services we access online - both at home and work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices and online. Staff need to change passwords regularly and ensure they are strong too. Two-factor authentication passwords are used for sensitive accounts such as CPOMS. They need to be careful which emails they access. If there are any concerns, staff know to report these to the Headteacher and IT support team.

When at home, staff need up-to-date anti-virus software to minimise the threats. Software updates increase the security of the computer. Children are taught skills on how to protect themselves too in as part of our computing scheme of work e.g. making passwords strong.

Social Media - Staff Code of Conduct

The school recognises and embraces the numerous benefits and opportunities that social media offers. While people are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

Definition of social media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, WhatsApp, Snapchat, Flickr and YouTube.

Employees should:

- Be aware of their online reputation and recognise that their online activity can be seen by others including parents/carers, pupils and colleagues on social media.
- Ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer.
- Be aware that any excessive use of social media in school may result in disciplinary action.
- Be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post

on a social networking site is something that they want pupils, colleagues, other employees, or even future employers, to read. If in doubt, don't post it!

- Not upload any content on to social media sites that is confidential to the school or its staff.
- Not upload any content on to social media sites that brings the school into disrepute.
- Not upload any content on to social media sites that is unlawful.
- Ensure live streaming is appropriate and doesn't breach any points in this policy.
- Phones should be stored away whilst on school premises.

Parental/Carers' requirements include:

- Not using their device for photos or videos during school events unless given permission.
- Not posting photos, videos or comments that include children at the school.
- Not using social media on their own devices while on school premises.
- Not accessing social media while helping at school or on school visits.
- Phones should be locked away whist on school premises.
- Raising queries, concerns and complaints directly with the school rather than posting them on social media – whether on their own pages, in closed groups (e.g. groups set up for school parents/carers to communicate with each other) or on the school's pages.
- Not posting anything malicious about the school or any member of the school community.
- Ensure live streaming is appropriate and doesn't breach any points in this Policy

Children are required to:

- Not join any social networking sites if they are below the permitted age (13+ for most sites including Facebook and Instagram).
- Tell their parents/carers if they are using the sites, and when they are online.
- Be aware how to report abuse and inappropriate content.
- Not access social media on school devices, or on their own devices while they're at school.
- Not to make inappropriate comments (including in private messages) about the school, teachers or other children.
- Be aware of the potential problems with live streaming and how to ensure their own safety.
- With potential unlimited access to data on mobile phones etc., children need to be aware of how to keep safe from dangers and to limit screen time.
- Be aware of their digital footprint because information about their online activity can be stored.
- Ensure live streaming is appropriate and doesn't breach any points in this policy.

Safeguarding

The use of social networking sites introduces a range of potential safeguarding risks to children and young people. Potential risks can include, but are not limited to:

- Online bullying.
- Grooming, exploitation or stalking.
- Exposure to inappropriate material or hateful language.
- Encouraging violent behaviour, self-harm or risk taking.

The 'Keeping children safe in education' DfE September 2024 outlines these four important areas of risk to consider:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group: https://apwg.org/

Reporting safeguarding concerns

- Any content or online activity which raises a safeguarding concern must be reported to the lead safeguarding officer in the school and recorded on CPOMS – Safeguarding Software for Schools.
- Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child.
- Personal safeguarding issues i.e. harassment or abuse received online while using work accounts should be reported immediately to the Designated Safeguarding Lead (DSL).

Potential and actual breaches of the code of conduct

In instances where there has been a breach of the code of conduct as outlined in this

policy, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy, this may result in action being taken under the Disciplinary Procedure.
- A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

Conclusion

Children and staff will be able to enjoy and use the school computers and tablets to:

- ✓ Enhance teaching and learning.
- ✓ Access useful educational information and materials, without risk of harm or upset