E-Safety Policy

Reviewed May 2024

Policy Approved by: _____

At meeting on: _____

E-Safety Policy

'We shine like stars to achieve and make a difference in the world, knowing that with God, all things are possible.'

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection. Our e-Safety Policy has been written by the school using government guidance. It has been agreed by senior management and approved by governors.

Security and data management

Keeping data secure

Sensitive data about pupils needs to be kept secure within school. This data needs to be kept secure at all times and it is the staff's legal responsibility to ensure that it remains safe whether it is being used inside or outside the school environment. When using and disposing of data staff must use the accepted means to store and dispose of the data.

Cloud storage

Recently the School's storage has started to move to the cloud. Our school is using Microsoft Office 365 and this means that staff can save documents to their password protected 'Onedrive' so that they can access this from anywhere.

Mobile devices and emerging technologies

The use of mobile devices

- School devices are allowed to take photographs and videos but personal devices are prohibited from doing so. School owns iPads and cameras to take these. Personal devices (such as cameras may be used if a school memory card is inserted into them and pictures are written to this)
- Staff mobile phones should, in accordance with the Child Protection Policy, be switched off, unless needed in an emergency.
- Images or videos of children or school must not be collected on staff mobile phones.
- In an emergency where a staff member does not have access to a school owned device, they should use their own device to telephone and hide (by inputting 141) their own device for confidentiality purposes.

Children's mobile devices

- If a child brings a mobile device into school it must go to the office to be kept securely and then be collected when the child leaves at the end of the day.
- If a child does have a mobile phone they are not to use it during school time, as in an emergency they can be contacted through the school office and a message can be passed to them.
- Images or videos of other children or the school must not be collected on the mobile device.
- Children are advised not to bring wearable technology into school, if this is brought into school it will be stored in the office until the end of the day when a

parent can pick it up. Staff are permitted to have wearable technology in school as long as it is used professionally and not during lesson times.

Emerging technologies
There are constant development and changes in both software and hardware in the field of computing. If a potentially suitable technology becomes available it will be tested and risk assessed to ensure there are genuine educational benefits and there are minimal risks. It will also be ensured that it meets with the law of copyright.

Digital Media

Consent
Written consent is provided by parents for the permission of media being used – this is in the GDPR Images Consent form.

Taking photographs/video
Member of staff are allowed to take pictures of children in educational use but only on school devices, they must not bring in their own camera or use their mobile phone. Staff members will use discretion when taking pictures to make sure the picture is not potentially embarrassing or the context of the picture could be misconstrued.

Parents taking photographs/video
In accordance with the Child Protection policy parents are allowed to take pictures of their own children. This must be for personal use and the image cannot be uploaded to social media such as Facebook or Twitter.

Storage of photographs/video
Photographs and videos will either be stored on the device or it will be stored on a computer/internal server which is password protected. Images are not stored in the cloud apart from the pictures on our assessment system, Arbor. When images are no longer needed they are to be deleted in line with our Retention Policy. Any physical copies of images will be shredded in the school office.

Communication technologies

Email
Staff should not use personal email accounts to communicate with service users. Staff should not use work email accounts for personal purposes.

Children in KS2 use Office 365 for internal email communication as part of the Computing curriculum.

Internet use
The school currently uses ‘Senso’ to monitor the appropriateness of internet usage. If a child or member of staff comes across an unsuitable website they are to inform the headteacher or e-safety coordinator immediately. Before children are allowed access to the Internet an acceptable use policy must be signed by the child, this is located in the child’s planner. Internet traffic through school will be monitored and it will be checked regularly to ensure that children and staff have acted sensibly and professionally.

Children will be taught what use of the Internet is acceptable and what is not, this will be done through Computing lessons and in other subjects, such as PSHE. They will also be taught how to find information on the internet safely and how to evaluate this information as well.

During Key Stage 1 children's use of the internet will generally be limited to teacher direction and occasionally they will be given an approved website that they can go onto.

Due to the ever changing nature of the Internet and the harm that can come to children topics such as radicalization and sexting will be discussed with the children. This will be done in a manner that does not upset or alarm the children, but in a way so that they know it is a risk to them. Children will be reassured that they can always speak to a member of staff if these incidents, no matter where the location.

Social networks
Social network websites are blocked on the schools filtering system and children, though the potential dangers of these will be taught to children.

Instant messaging/VOIP
Most of these services, such as Skype and Facetime, are blocked through the schools filtering system however if they are used in school the risks will be assessed and communication will only be to approved sources e.g. staff members or other children.

Dealing with incidents
Incidents can either be illegal or inappropriate. Generally in school it will be inappropriate incidents that will need to be dealt with.

Illegal incidents
If an illegal incident occurs, the member of staff will contact the Headteacher who will then contact the LA. If necessary the Police, CEOP or the Internet Watch Foundation would be informed.

Inappropriate incidents
If an inappropriate incident occurs staff will inform the Headteacher and the e-safety coordinator who will decide on the best course of action. Examples of inappropriate incidents and their consequences are:

Incident	Procedure and sanction
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off. • Tell a trusted adult. • Report to Headteacher and complete Incident Log.

	• Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform Headteacher or designated e-safety Coordinator • Enter the details in the Incident Log. • Additional awareness raising of e-safety issues and the AUP with individual/child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

The incident log can be located in a secure place in the Headteacher's office.

<u>Education and training</u>

Both staff and children need to be taught how to be digitally literate so that they minimize their risk to themselves and others whilst online. Ofsted have said there are 3 main risks when using computers.

These are:

Area of Risk	**Example of Risk**
Content: Children need to be taught that not all content is appropriate or from a reliable Source.	• Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence) • Lifestyle websites. • Hate sites. • Content validation: how to check authenticity and accuracy of online content.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming • Cyber bullying in all forms • Identity theft (including hacking Facebook profiles) and sharing passwords.

Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	• Privacy issues, including disclosure of personal information, digital footprint and online reputation • Health and well-being - amount of time spent online (internet or gaming). • Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Children will be taught about these risks throughout school. These will be through materials from the 'thinkuknow' website. This provides age appropriate materials covering things like keeping passwords, not giving out personal information, how to keep safe if you do use social networks and cyber bullying. These materials are age progressive and ensure that age relevant risks are discussed with the children. Again, children will be taught about the more recent risks of sexting and radicalization in age appropriate ways.

E-safety rules
Rules to keep safe will be displayed in each classroom as a visual reminder on how to keep safe whilst using computers.

Staff awareness
Staff will be given this document followed by a staff meeting on this subject to ensure that all staff understand how vital e-safety is in school, any training issues that arise from this meeting and skills audit will be addressed either internally or through courses.

Prevent duty
Aspull Church Primary School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.

We protect children from the risk of radicalisation, for example by using filters on the internet to make sure they can't access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.

Our Safeguarding, Prevent Duty and e-safety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.

Parental awareness
"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Parents will be given access to a copy of this policy and will be offered regular workshops to help parents understand the risks that their children face when using devices.

Policy Decisions

Authorising Internet access

Parents will be asked to sign and return a consent form that authorises children to access the internet.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The school will audit IT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.