Dalton St. Michael's C.E. Primary School

E-Safety Policy

E-Safety Policy

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- The school has an appointed e-Safety Coordinators – Mr Attkins and Mrs Robinson.
- 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. LCC have bought into Office 365 and this means that staff can save documents to their password protected 'Onedrive' so that they can access this from anywhere. The School widely uses this in relation to the Learning Journeys in the Early Years Foundation Stage. This is used with the orbit app of the iPad. It has been ensured that orbit safeguards information safely and securely and that it follows all necessary procedures set out by the government. The data from this is stored in the cloud and once the app has been closed on the iPad it deletes all of the data and photographs taken on the iPad.

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.
- Images or videos of children or school must not be collected on staff mobile phones.
- When on trips or out of school there is a school mobile phone that staff are able to use to contact school and parents if needed.

- Apart from educational devices no device must be connected to the school's Wi-Fi.

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.
- An exception to this is dedicated eBooks e.g. Kindles. In the Upper Juniors if the children own one, they are allowed to bring it in to read it during silent reading time. If a child brings an eBook into school it is **their responsibility** to keep it safe. Although tablets like iPads have readers on them these are not acceptable
- 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 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 photographs being taken of their children and this permission also regulate whether children's images and/or names can be used in 3rd party publication or the school website.
The permission also includes the acceptance of their child having their photo being taken in a group shot and then their image being used for another child's Learning Journey

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 devices memory stick and this will not be taken outside of school. Or it will be stored on a computer which is password protected or on the school's internal server. Pictures of children and school should not be stored on staff's USB sticks as they will more than likely be taken outside of the school setting and most cannot be encrypted/password protected.
Images are not stored in the cloud apart from the pictures in the Early Years Foundation Stage orbit app. These are stored securely on orbit's secure servers at an undisclosed site. When images are no longer needed they are to be deleted and checked that they are gone and physical copies of images will be shredded in the office.

Communication technologies

Email
Currently children do not have a school email account, if this were to change in the future the school would do it through the Office 365 subscription and the risks of email and best practices would be taught to the children. Practise can be done via the purple mash website, all children have a login for this.

Internet use
The school use BT Lancashire Light Speed to filter internet traffic and websites like blogs, journals and social networking are automatically blocked. If a child or member of staff comes across an unsuitable website they are to inform the e-safety co-ordinator immediately. Before children are allowed access to the Internet a permission slip but be handed into school and an acceptable use policy must be signed by the child.
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.
When children are researching on the internet they must start with www.swiggle.org or www.kidrex.org. This is a website that automatically customizes the search so that it has the highest level of filtering. If information cannot be found on that then children can use Google but before they use it staff will look at the results on their computer to ensure no inappropriate results will be forthcoming.

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 LCC. 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/click the 'Hector Protector' button. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • 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
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	

Using chats and forums in an inappropriate way.	offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.

The incident log can be found in the appendices and will also be located in a secure place in the Headteacher's office.

Education and training

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. These can also be found in the appendix.

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.

Staff and Governors have completed training with regards to the Government's PREVENT strategy from the Lancashire Police. They understand how to report concerns and what type of behaviour to look for.

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 a copy of this policy and in the future there will be workshops to help parents understand the risks that their children face when using devices.

Policy Decisions

Authorising Internet access

- The school will keep a record of all pupils who are granted Internet access. The record will be kept up-to-date.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

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 ICT 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.

Signed:	Signed: On behalf of the Governing Body
Head Teachers name: Mrs Adele Robinson	Chair of Governors name: Mrs Maureen Faulkner
Date: January 2017	Proposed Review date: January 2018

Appendix

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen and when an adult is around.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail or communicate with people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We only use programmes and content that has been installed by school.

Date/time of incident	Type of incident	Name of pupil/staff involved	System details	Incident details	Resulting actions and by whom (signed)
21/10/2013 11.42	Accessing inappropriate website	AN Other (pupil) AN Staff (staff)	Laptop 3	Teacher observed child deliberately trying to access adult websites	Pupil referred to Headteacher and given warning in line with sanctions policy for 1st time infringement of AUP. Site reported to LGFL as inappropriate.