**E-Safety Policy**

**Aims**

This policy applies to all staff, governors and pupils, as well as others who have access to or use the school’s IT system, both in and out of the school setting.

**The purpose of this policy is to:**

* Set out the key principles expected of all members of the school community at Meanwood with regards the use of ICT-based technologies.
* Safeguard and protect the children and staff.
* Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
* Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
* Have clear structures to deal with online abuse such as cyberbullying.

**Areas of Risk.**

The school aims to make children aware of, and educate them, on the dangers presented by technology and how they can manage their own safety.

**The main areas of risk for our school community can be summarised as follows:**

### Content

* Exposure to inappropriate content.
* Content that promotes ideology contrary to the ethos of the school, British Values or acceptable behaviour.
* Inaccurate or unauthentic content.

### Contact

* Grooming
* Cyber-bullying in all forms
* Identity theft and sharing passwords

### Conduct

* Privacy issues, including disclosure of personal information.
* Digital footprint and online reputation.
* Health and well-being (e.g. amount of time spent online)
* Showing respect for copyright.

**Meanwood e-safety Curriculum**

To minimise the risks posed by the above areas this school has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA and Government guidance as well as the e-safety aspect of the National Curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

* + The Zip it, Flag it, Block it approach.
  + Developing their ability to analyse and verify the accuracy and authenticity of information online.
  + Build awareness that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
  + To know how to narrow down or refine a search, use search engines efficiently and know how to use ‘safe searches’.
  + To understand how search engines work and to understand that this affects the results they see at the top of the listings.
  + To understand acceptable behaviour when using an online environment
  + To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
  + To understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments.
  + To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos.
  + To understand why they must not post pictures or videos of others without their permission.
  + To know not to download any files – such as music files - without permission.
  + To have strategies for dealing with receipt of inappropriate materials;
  + To understand the impact of cyberbullying and trolling and know how to seek help if they are affected by any form of online bullying.
  + To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

**Staff and governors.**

This school

* Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
* Makes regular training available to staff on e-safety issues and the school’s e-safety education program.
* Provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the e-safeguarding policy and the school’s Acceptable Use Policies.
* Requires staff to avoid making reference to school/pupils/parents or other staff on social media in relation to their job or giving personal opinions on any of the above on social media.
* Requires staff to check their privacy and security settings regularly to reduce the chance of personal information or data loss.
* Ensures staff know not to use personal electronic devices to store or capture data in school (including pictures of children or their data). School provides secure devices for this e.g. staff laptop, encrypted hard drives and school cameras.

**Parent awareness and training.**

This school runs a rolling programme of advice, guidance and training for parents, including:

* Introduction of the annually reviews Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear.
* Information on the school web site.
* Workshop sessions held at school.
* Suggestions for safe Internet use at home.
* Provision of information about national support sites for parents.

Parents are also encouraged to raise any concerns or difficulties with an adult in school who will involve the necessary members of staff (see table below).

**Responsibilities for E-Safety**

Below is a table detailing the responsibilities of members of the school community as regards to the implementation of the e-safety policy.

| Role | Key Responsibilities |
| --- | --- |
| Headteacher | * To take oversee the work of other staff with regards to e-safety provision. * To take overall responsibility for data and data security (in liaison with the School Business Manager and Computing team). * To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements (in liaison with the School Business Manager and Computing team). * To be aware of procedures to be followed in the event of a serious e-safety incident (i.e. an event which breaks the law or exposes children to any form of abuse). * To receive regular monitoring reports from the Computing team. |
| E-Safety Co-Ordinator/ Computing Lead. | * To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. * To be responsible for ensuring the profile of E-Safety is high and high quality teaching is delivered regularly throughout the school. * To build parent-school relationships and educate parents and other partners with regards to E-Safety. * To review the E-Safety policy on an annual basis. * To take day to day responsibility for e-safety issues. * To liaise with ICT support staff. * To communicate with SLT and governors. * To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. |
| Governors /  E-safety governor | * To ensure that the school follows all current e-safety advice to keep the children and staff safe. * To approve the E-Safety Policy and review the effectiveness of the policy. * To support the school in encouraging parents and the wider community to become engaged in e-safety activities |
| Network Manager/technician in liaison with School Business Manager and the Head. | * To ensure all systems and data are protected to the correct standard. This includes encryption, ensuring passwords are set and used and data protection protocols. |
| Teachers | * To embede-safety issues in all aspects of the curriculum and other school activities. * To supervise and guide pupils carefully when engaged in learning activities involving online technology. * To follow the school policy on e-safety and safeguarding. * To deliver the e-safety curriculum. |
| All staff | * To read, understand and help promote the school’s e-safety policies and guidance * To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. * To report any suspected misuse or problem to the e-safety coordinator. * To maintain an awareness of current e-safety issues and guidance e.g. through CPD * To model safe, responsible and professional behaviours in their own use of technology * To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. |
| Pupils | * To read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy. * To take responsibility for their use of the Internet and other technologies by using them safely both in school and at home. |
| Parents/carers | * To support the school in promoting e-safety and endorse the Pupils’ Acceptable Use Agreement which includes the pupils’ use of the Internet and the school’s use of photographic and video images. * To consult with the school if they have any concerns about their children’s use of technology |
| Authorised Visitors | * Any external individual / organisation agrees to follow the e-safety policy which will be signposted on their induction sheets provided by the office. |

**Policy Breeches.**

The school will make all reasonable efforts and take all necessary precautions to ensure children are kept safe on-line. Whilst the attitude of users is generally positive and there are rarely incidents, in the event that school policy is not followed these actions may be taken:

* action will be taken to rectify and monitor the e-safety incidents in line with the school’s behaviour policy (see separate policy).
* In exceptional circumstances it may be necessary to involve outside agencies.
* Incidents of cyberbullying will be dealt quickly, sensitively with in accordance with our Anti-Bullying Policy and in partnership with parents and carers.
* E-safety incidents that prompt a child protection concern are dealt with in accordance with school / LA child protection procedures.
* Records are kept of e-safety incidents that incur a slip. These are monitored by the e-safety coordinator and the Head in conjunction with the designated governor for e-safety.
* Parents and carers are informed of incidents.
* School policy is to contact the Police if any of our staff or pupils receives online communication that is particularly disturbing, offensive or breaks the law.

Allegations against staff will be dealt with by the Headteacher and/or Governors following school disciplinary procedures.

**Risk Assessment.**

Specific risks can arise from the use of different technologies in school. Below is a risk assessment and the procedures all staff and pupils agree to follow to minimise those risks.

|  |  |  |
| --- | --- | --- |
| **Situation** | **Risk** | **Procedure** |
| Equipment (including iPads, cameras and laptops) stolen/lost | Potentially sensitive data is lost (e.g. children’s pictures) | * iPads and laptops are to be kept locked in their cases overnight (KS1 staffroom or KS2 PE cupboard for iPads). * iPads and portable devices like cameras are not to be left out on view in classrooms at the start or end of the day when the school site is less secure. * Data, particularly pictures of the children, should be deleted off the iPads at the end of the unit of work. * iPads are not to be taken off site on school trips etc. * If staff need to use an iPad at home for lesson planning it must be checked first and any sensitive data removed as they are not password protected. * Staff agree that their personal home or car insurance covers any school equipment in their possession outside of school. * Staff agree to follow the home use of school laptop agreement. * iPads used to store children’s information (such as those used by EYFS and Yr1 staff) will be PIN protected. |
| Damage to the computing equipment | * Cuts from broken screens/cases. * Electric shocks. * Cost implications. | * iPads are kept in protective cases. * Staff should judge the age and nature of the child before allowing them to use equipment unsupervised. * Equipment should only be used outside with adult supervision. * Only one child should hold the unit or touch the screen at once. * Broken iPads or other equipment need to be handed in to a member of the computing team. |
| Changing settings on the iPads | * Security/ privacy settings are altered exposing children to unsuitable material. | * Settings features are kept within the ‘teacher’ icon on the iPad. * Children agree not to use this function. * Staff should consult with a member of the computing team if they are unsure of any of the settings or functions of the iPad. |
| Loss of pictures from school cameras. | Potentially sensitive data is lost. | * Pictures should be removed from camera memory cards and stored on the O:Drive or the year group’s encrypted hard drive as soon as practical. |
| Filter failure/ inappropriate websites | Children can be exposed to inappropriate content. | * If anything becomes available that shouldn’t on children’s devices staff should inform a member of the computing team immediately who will liaise with the service provider to update the filter. |
| Overheating/ damage to batteries | Equipment is damaged  Fire hazard | * Devices must not be left on charge overnight. |

Policy reviewed June 2020