Inspiring Futures Partnership Trust

# INSPIRING FUTURES PARTNERSHIP TRUST

# E-SAFETY POLICY

| | |
|---|---|
| Policy Type | Curriculum/Child Protection |
| Updated By | Victoria Morris |
| Updated in | July 2018 |
| Next review | July 2019 |
| Reviewed | Annually |
| Website | Yes |

# Inspiring Futures Partnership Trust

## E-SAFETY POLICY

### Policy for E-Safety and Acceptable Usage

Within the Inspiring Futures Partnership Trust, we recognise the importance of using, and developing a good understanding of new technologies to enhance learning. Moreover we are aware that the technology will play a fundamental part in the present and future lives of our children and that ICT in our schools should reflect ICT in society.

The trust is committed to the developing ICT in order to create ICT users with the skills necessary to quickly adapt to new technologies, as well as creating effective communication between pupils, staff, parents and the wider community to share our trust news.

However, as in any other area of life, we are aware that children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. E-Safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

**Network Safety:**

- All users need to log on using their username, this is specific to them. The children are taught from EYFS that they should only log on using their own username.
- Each user is given an allocation of disk space for the storage of their work. Pupils are taught how to save their work into their “My documents” area; however they are encouraged to only save the work they need to and not to save too many pictures and large files.
- Access to other users’ “My documents” areas are restricted by the network. Pupils are taught not to access another user’s work without permission.
- On networks there is a ‘Whole School Shared’ area where many different groups of users can save work so that it is available to others. Pupils are taught how to access the shared area, however we expect pupils to be respectful of other people’s work and not to delete anything without permission.
- Pupils are only allowed to print their work under the instruction of an adult. Work prints to the networked photocopier.
- Children will be taught not to change or alter any settings. Although children are unable to access a large part of the network, they still need to be taught the importance of this.
- Only the network administrators are permitted to install software on to the networks. Staff requiring additional software must log a support call to be dealt with by the ICT administrators. If apps are required for the tablets or other mobile devices, staff need to ask the ICT tech support; if these are paid apps, permission must be sort from the subject specific budget holder, for example maths**.**
- All users of the networks can be monitored remotely by the network administrators. *Pupils are taught that their use of the network can be monitored.*

**Internet Safety:**

- E-Safety is included as an ICT teaching unit in every year group, ensuring that children understand the dangers of the internet and how to keep themselves safe , progressing at an age-appropriate rate. It also features in some PSHCE lessons.
- The systems within the trust academies are filtered by the internet provider for the safety of the children and staff. These filters are designed to protect the children and staff from accidental or deliberate access of unsuitable materials. The network administrators can manually block site addresses which are considered unacceptable, or unblock those sites which are acceptable and have been incorrectly blocked. DSLs perform occasional checks on searches to ensure that this is working effectively.
- No system is 100% safe and we expect users to behave responsibly. Pupils are taught that the internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or can damage your computer. Children are also taught that whilst the internet is useful, not everything on the internet is true and that children need to use trustworthy sources and websites.
- Children are taught to report to the nearest adult, immediately, anything that they see which they find upsetting, inappropriate, or which they believe should have been blocked by the filtering system. All reports of this nature will be logged on CPOMS, the trust safeguarding software.
- We teach pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games, other media or social networking sites.
- Pupils accessing the internet at home are subject to the controls placed upon them by their parents/carers. However, any home use of the internet made in connection with the trust or its academies' activities; any of its staff, pupils and trustees or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at academy. We expect all members of our trust community to behave as positive ambassadors of the trust and its academies in all academy/trust related activities made through the internet.
- The trust academy websites contain academy policies, newsletters and other information. **We expect all persons accessing the academy websites to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the academy.**

**Email safety:**

Some pupils will have their own webmail accounts at home. As these are independent of the academy they do not necessarily come with the safeguards that we set for email usage. Therefore we do not permit the use of personalised email accounts by pupils at the academy or at home for academy purposes. Most personal email websites are blocked by the trust academies' web filtering systems, however there is the possibility that some may not be.

**Website safety:**

Children are taught that they need to also be very careful when using online sites. They should **never give their real name, school, age or location.** Children are taught the

dangers of: giving out personal information to strangers on the internet such as phones numbers, school name, personal photos or addresses. Children are also taught that the people that they are communicating with may not be who they think they are – people can lie online. Each year group teaches a topic relating to online CSE at an age-appropriate level- content includes identifying 'too good to be true' offers, over-flattery, attempts at manipulation etc.

**Digital Images:**

- Digital cameras are used for recording events on video and photo as well as being essential tools for everyday learning experiences across the curriculum. When children arrive at a trust academy, all parents/carers are given the Trust use of images opt in form. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the trust or academy website, the closed academy Facebook group or Twitter account. Online, we will never state a child's full name with their image. The trust academies will happily remove any image of a child on the academy website at their parent/carer's request.
- Digital images may be shared with partner schools and organisations as part of collaborative learning projects or training. This can include live video conferencing. All such use is monitored and supervised by staff. Pupils are taught to seek permission before copying, moving, deleting or sending any images taken within the trust academies. We expect all pupils to seek permission from staff before sharing images outside of the trust academies environments.
- **Staff may not take photos of the children in any state of undress or in swimwear. (Please refer to the Trust staff acceptable use policy with regards to the trust academies' cameras or devices with the ability to capture images, videos or audio recordings).**

**Usernames and Passwords:**

- Children have usernames and passwords for the network and for different online software packages. They are taught not to reveal these to anyone aside from their parent/carers. They understand that staff keep a copy of these securely in order to protect them any incident of E-Safety and also to allow the child access when they may have lost or forgotten their username or password. Children must never be allowed to log on as someone else. (Please refer to the staff acceptable use policy for staff passwords and accounts).

**Cyber Bullying:**

- The trust takes all forms of bullying very seriously. Cyber-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Pupils are taught about bullying, including cyber-bullying as part of the PSHE curriculum. We expect all members of our community to communicate with each other with respect and courtesy. Cyber-bullying will be dealt with under the procedures within the Trust Policy on Behaviour**.** All incidences of cyber bullying are recorded on CPOMs, the Trust safeguarding software. Cyber bullying which takes place outside of academy hours, if reported by a pupil or parent/carer, will be dealt with as far as is reasonably possible by trust staff.

**Mobile Phones:**

- Pupils are not permitted to have mobile phones in the trust academies. If a phone is brought into a trust academy, it will be confiscated by a member of staff and only returned to an adult. (Please refer to the trust staff acceptable use policy with regards to mobile phones that belong to staff).

**Other technologies:**

- **Podcasting** – Some pupils will be given opportunities to create oral recordings. Some of these recording may be made available as podcasts through the internet so that they can be shared with interested members of the trust community, first names only may be used.

**Use of electronic communication and recording devices (ECRD):**

- **ECRD** includes any device with the capability to capture or record audio, photograph or video or is capable of receiving or transmitting any type of communication between persons.
- The trust believes that pupils, academy staff, volunteers, visitors and trustees should not be subject to having a video or audio recording taken of them without their consent. This aspect of the E-Safety policy protects their rights to privacy. This means that volunteers, visitors, parents/carers and pupils are not allowed to bring ECRD into the Academy for the purpose of use them for capturing audio, photographs or video of any person without having obtained that person's consent and the permission of the Principal.
- The trust gives permission for parents/carers (as a member of the audience) to use an ECRD during whole school or class performances or productions. Any parent or carer has the right to ask for their child to be removed from a production or performance if they do not wish for their child to potentially be recorded in the process of a group recording. The trust requests that parents do not upload group shots of pupils to social media without the other parents' permission.
- The Trust does permit the use of ECRD devices by academy staff only in school for the purposes of school based teaching and learning. The use of these ECRD devices is closely monitored by the academy heads of school/principals. Use of any audio, photograph or video captured outside of the academy is subject to permission having been granted by each pupil's parent or carer on the trust opt in form (a copy of which will be held on the Academy's records).

**Child protection:**

- Any E-Safety incident which raises concerns about a child protection issue will be reported to the school Designated Safeguarding Leads and referred to Social Care as appropriate. It will be recorded on the trust safeguarding software, CPOMs.

## E-Safety Rules for KS1

**Key Stage 1**

| |
|---|
| I only use the internet when an adult is with me. |
| I can search the Internet with an adult. |
| I can send and open emails with an adult. |
| I never tell anyone except my parents my password. |
| I know that my teacher has a copy of my username and password in case I forget it. |

## E-Safety Rules for KS2

**Key Stage 2**

| **Think then Click** |
|---|
| E-Safety Rules for Key Stage 2: |
| . I am not allowed mobile phones in school.<br>. I ask permission before using the Internet.<br>· I only use websites that an adult has told me are safe.<br>. I do not search the internet for things that I know adults would not like me to look at.<br>. I understand that I will not be allowed to use the internet if I break any E-Safety rules.<br>· I will tell an adult if I see anything I am uncomfortable with.<br>· I will immediately close any web page I am not sure about.<br>· I will only e-mail people an adult has approved.<br>· I will only send e-mails or post messages that are polite and friendly.<br>· I will never give out my name or any personal information or passwords.<br>. I know that my teacher has a copy of my usernames and passwords in case I lose or forget them.<br>. I am always myself and do not pretend to be anyone or anything I am not while online.<br>. I will not use the internet in a way which may harm or cause upset to others.<br>. I know that my teacher and the Internet Service Provider will check sites that I have visited.<br>· I will never arrange to meet anyone in person through the internet.<br>· I will not open e-mails sent by anyone I don't know.<br>· I do not use Internet chat rooms.<br>. I will not put or send pictures of myself on the Internet. |

---

**For further details please download our E-Safety policy on the academy website:**
http://www.cheppingviewprimaryacademy.org/Policies

**E-SAFETY**
**Please sign and return.**

I confirm that I have read the academy's E-Safety rules and the E-Safety policy and discussed it with my child

Parent/Carer name: _____ Signed: _____

I have read the E-Safety rules and I have talked about them with my family. I will follow them at all times:

Child's name: _____ Class: _____Signed: _____

Updated July 2018