# E Safety Policy

**Introduction**

Tankersley C of E Aided Primary School fully recognises its responsibilities for safety, incorporating e-safety, within school.

E-Safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, tablets, collaboration tools and personal publishing.

The school's e-safety policy will operate in conjunction with other policies and Protocols including:

- Behaviour policy
- Anti-Bullying
- Child Protection and Safeguarding
- Data Protection and Security
- Media log – parental permissions

With an increasing use of technology in school, e-safety is a vital part of the wider, curriculum. E-safety is delivered through assemblies by the Computing subject lead and through the wider curriculum. A dedicated themed week for e safety takes place in school annually and the children discuss safety as part of this and up to date information is disseminated across school. Posters are up in the computer room and around school reminding the children about e-safety.

Protocols for breach of the schools esafety guidelines and protocols are included in the policy.

See formats at the end of this document for reporting any incidents and for a copy of the staff proforma which is signed by staff to ensure safe conduct on electronic devices.

**Aim**

The aim of this policy is to provide guidance for the prevention of and management of E-Safety incidents within school. It is a complimentary document to the Safeguarding policy.

**Definitions**

*E-Safety* – Knowledge and understanding of risks on the internet or other online areas and an understanding of how to manage these risks.

*Social Media* -Websites and applications that enable users to create and share content or to participate in social networking.

*Sexting* - Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages.

*YPSI* – Youngsters Preparing Sexual Imagery – Taking and distributing photographs by students under 18 years old.

*Pornography* - Printed or visual material containing the explicit description or display of sexual organs or activity, intended to stimulate sexual excitement.

**National Requirements**

- Key stage 1 – children should use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content to contact on the Internet or other online technologies
- Key stage 2 – use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concerns about content and contact

*(National Curriculum 2014)*

**E Safety Co-ordinator - Roles and Responsibilities**

**Key responsibilities of the eSafety coordinator include:**

- Developing an e-Safety culture acting as a named point of contact on all eSafety issues
- Leading and promoting the e safety vision to all stakeholders/members of the team and supporting them in their understanding of the issues
- Ensure that e-Safety is embedded within the continuing professional developments for staff and co-ordinate training as appropriate
- Ensure that e-safety is embedded across the curriculum and activities within the organisation as appropriate
- Ensure that e-Safety is promoted to parents and carers, and other users of network resources
- Maintain an e-Safety incident log
- Monitor and report on e-Safety issues to the management team, other agencies and the local authorities e-Safety lead as appropriate
- Develop an understanding of the relevant legislation
- Liaise with the local authority and other local bodies as appropriate
- Liaise with other agencies as appropriate

## Social Networking Use

Social networking applications include, but are not limited to:

1. Social Networks (e.g. Facebook)
2. Bookmarking sites (e.g StumbleUpon)
3. Social News (E.g Reddit)
4. Media Sharing (e.g Youtube)
5. Microblogging (e.g. Twitter)
6. Blog Comments and Forums

Staff and students must not access social networking sites for personal use via school information systems, school networks or using school equipment

- If staff access social networking sites using their personal computer systems and equipment, they should never give out personal information of any kind which could identify themselves, colleagues and / or pupils as staff at Tankersley.
- Staff must not place inappropriate photographs on any social network space and must – where they do post photographs - ensure that background detail (eg house number, street name, school) cannot identify them
- No photographs are to be posted of school activities or within the school grounds unless through school website.
- Staff are not to communicate or "friend" students within the school
- Former students and parents of students are to only be added after notifying the Head teacher or other member of the Senior Leadership Team
- All parents and student's currently "Friended" on social media must be removed on signing of this policy unless exemption given by the Head teacher
- Staff must not run social network spaces for student use on a personal basis
- Schools are vulnerable to material posted about them online and all staff should be made aware of the need to report this should they become aware of anything bringing the school into disrepute. Schools are advised to check regularly, using a search engine, to see if any such material has been posted
- f staff use social networking sites they should not publish specific and detailed "personal views" relating to the Agency, its schools, staff or students.
- Breaches of these regulations will lead to disciplinary action9
- The school network and Computing facilities must not be used for the following activities:
- Conducting illegal activities
- Accessing or downloading pornographic material
- Gambling
- Soliciting for personal gain or profit

- Managing or providing a business or service
- Revealing or publicising proprietary or confidential information
- Representing personal opinions as those of the Agency or its schools
- Making or posting indecent or offensive remarks or proposals

## Incident Management Process for breaches of eSafety Policy

| Action to be taken when the breach is made by a member of staff | Person Responsible |
|---|---|
| Where there is concern that there has been a breach of the eSafety Policies and inappropriate sites have been accessed the person who is made aware of this will report this to the agencies designated lead for eSafety/safe guarding | Member of Staff aware of the incident |
| The designated lead in the agency will conduct an initial fact finding investigation which will ascertain who was involved, what sites have been accessed. The laptop/computer will be withdrawn immediately and placed in a safe and secure place | Designated Lead |
| The designated lead will classify the incident appropriately (high or low severity) and enter details of the incident into the agencies incident log | Designated Lead |
| The head teacher/line manager will have been informed and should be given the results of the initial fact finding investigation | Designated Lead |
| The head teacher/line manager will discuss the concerns with the Local Authority Designated Officer (LADO) in order to discuss whether there is a need for a Strategy Meeting. During this discussion consideration will be given as to whether the police need to be involved. The head teacher/line manager will also discuss with their HR advisers if the member of staff needs to be suspended or undertake different duties pending the completion of the enquiries. | Head Teacher/Line Manager |
| The line manager/head teacher will also discuss the incident with the eSafety lead in the Local Authority as consideration will need to be given to any further actions required. | Head Teacher/Line Manager |
| Discussions will also need to take place between the local authority eSafety lead and Strategic COMPUTING lead to agree if the site(s) are blocked for the duration of the investigations. | eSafety Lead |
| The strategy meeting process will be completed following the South Yorkshire Child Protection Appendix 4 Allegations Against Staff Protocol www.safeguardingchildrenbarnsley.gov.uk | |
| The designated lead will complete the agencies incident log and send a copy to the Local Authority's eSafety lead | Designated Lead |

| | **Action to be taken when a *young person* has been accessing inappropriate sites** | **Person Responsible** |
|---|---|---|
| | Where there is concern that there has been a breach of the eSafety Policies and inappropriate sites have been access the person who is made aware of this will report this to the agencies designated lead for eSafety/child protection | Member of Staff aware of the incident |
| | The designated lead in the agency will conduct an initial fact finding investigation who will ascertain who was involved, what sites have been accessed. The laptop/computer will be withdrawn immediately and placed in a safe and secure place | Designated Lead |
| | The designated lead will classify the incident appropriately (high or low severity) and enter details of the incident into the agencies incident log | Designated Lead |
| | The head teacher/line manager will have been informed and should then be given the results of the initial fact finding investigation | Head Teacher/ Designated Lead |
| | The head teacher/line manager will discuss the concerns with the manager of the Assessment Team in their area to establish if there are child protection concerns requiring a Section 47 Child Protection investigation. If this is required the Assessment Team will conduct this investigation as required within the South Yorkshire Child Protection Procedures | Head Teacher/Line Manager Assistant Team Manager |
| | If there is no child protection investigation a decision will be made between the head teacher/line manager and the duty social worker as to whether additional work will be completed with the young person and their family via an Initial Assessment or the Common Assessment Framework. This process will ensure that parents are fully aware of the concerns/incidents and they will be given advice and information about managing the internet, use of parental controls etc. | Assessment Team |
| | At the time that the incident is reported the computer/laptop will be removed. The eSafety lead in the agency will ask Code Green/ the brokered IT supplier to investigate what has been accessed on the hard drive and will be asked to complete a report detailing the usage. This report will be made available to the agency, Strategic COMPUTING and the lead for eSafety in the authority. This report will be required to inform the investigations. | eSafety Lead/Code Green IT/Brokered IT Supplier |
| | The management of eSafety within the agency will also need to be considered including any recommendations for additional training | |
| | After the completion of all investigations the head teacher/line manager will need to provide a report to the Local Authority lead/Strategic COMPUTING to outline the outcome of the work undertaken, updated risk assessments relating to the management of access to computers any identified training needs. | |
| | Discussions will take place based on the information available to decide whether it is appropriate for the site(s) to be unblocked and Strategic COMPUTING will arrange the unblocking of the site and the notification to the agency/other agencies that also need access to the site. | Strategic COMPUTING eSafety lead |
| | The designated lead will complete the agencies incident log and send a copy to the Local Authority's eSafety lead | Designated Lead |

**TANKERLSEY C OF E (A) PRIMARY SCHOOL**
**Staff Code of Conduct for use of electronic devices and E safety**

**To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.**

- I understand that it is a criminal offence to use a school Computing system for a purpose not permitted by its owner.
- I appreciate that COMPUTING includes a wide range of systems, including mobile phones, IPADS, PDAs, digital cameras; email, social networking and that COMPUTING use may also include personal COMPUTING devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I have read, understood and accept the Staff Code of Conduct for COMPUTING.

Signed: …… Date: ……

**TANKERLSEY C OF E (A) PRIMARY SCHOOL**

## PUPIL GUIDELINES FOR SAFE INTERNET USE AGREEMENT

- **I will only use the Internet when there is a teacher or TA present.**
- **I will only use the computers and websites that pupils are allowed to use with permission**
- **I will always ask for permission before accessing the Internet/email.**
- **I will only use my own usernames and passwords to log on and keep them secret.**
- **I will not access other people's files or folders.**
- **I will only email or contact people I know, or my teacher has approved; and ensures that the messages that I send will be polite and responsible.**
- **I understand that the use of strong language, swearing, bullying or using inappropriate pictures is not allowed**
- **I will not give out personal details (like my home address, telephone or mobile number), or the personal details of any other person to anyone, or arrange to meet someone unless my parent/carer or teacher has given me permission.**
- **I will only view, download, store or upload material that is lawful, and appropriate for other users. If I am not sure about this, or come across any inappropriate materials, I will inform my class teacher straight away.**
- **I will ask to delete anything or move files from a school computer**
- **I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.**

| | | | |
|---|---|---|---|
| **Pupil's Name** | | **Class Teacher** | |
| As a school user of the Internet, I agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school. | | | |
| **Pupil Name (print)** | | | |
| **Pupil Signature** | | **Date** | |

**PLEASE NOTE – ALL PUPILS FROM Y2 TO Y6 NEED TO SIGN THIS SAFETY AGREEMENT IN SEPTEMBER ANNUALLY**

**PUPILS IN EYFS AND WILL HAVE THIS SIGNED BY THE CLASS TEACHER FOLLOWING A DISCUSSION APPROPRIATE TO THEIR AGE**