E-Safeguarding Policy

1. Teaching and Learning

1.1 Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2 Internet use will enhance learning

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2. Managing Internet Access

2.1 Information system security

All school computers will have Sophos antivirus installed to protect the network from virus infections. Sophos automatically updates and scans the computers.

2.2 E-mail

Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
E-mail sent to an external organisation should be written carefully and authorised before sending.

2.3 Published content and the school VLE

Staff or pupils' personal information will not be published.
The head teacher and ICT co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

2.5 Social networking and personal publishing

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school pupils or parents, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in school requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting images that are discriminatory or offensive or links to such content.

2.6 Managing filtering

The school uses a filtered internet service provided by Yorkshire and Humberside Grid for Learning (YHGFL). The filter provided by YHGFL will stop most unsuitable searches or content being found, this includes inappropriate games, images, websites and links to radicalisation and extremist content in line with the Prevent Duty.

If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator (ICT Co-ordinator) Mr Paine. The school will report this to the appropriate agencies including the filtering provider and record onto the appropriate safeguarding forms in accordance with the safeguarding policy.

2.7 Managing emerging technologies

Device	Pupils	Staff
Mobile Phones	Not allowed	Staff allowed
Taking photos or videos on school equipment	Pupils allowed supervised by an adult	Staff allowed
Use of hand held devices such as personal gaming consoles	Not allowed – only during golden time	Staff allowed
Use of personal email addresses in school	Not allowed	Staff allowed on school owned laptops.
Use of school email address for personal correspondence	Not allowed	Staff allowed
Use of online chat rooms	Not allowed	Not allowed
Use of instant messaging services	Not allowed – only within school VLE with monitored checks	As pupils
Use of blogs, wikis, podcasts or social networking sites	Not allowed – only within school VLE with supervision and monitoring	As pupils
Use of video conferencing or other online video meetings	Not allowed – apart from those set up by and supervised by staff	As pupils
School IPads	Allowed, but need to be monitored by adults and directed to specific apps.	Staff allowed, adhering to the school acceptable computing use agreement.

2.8 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
Staff will ensure they properly log off from any computer after accessing personal data.
Staff will not remove personal or sensitive data from the school premises without permission of the head teacher and without ensuring such data is kept secure.

2.9 Data storage

- Staff are expected to save all data relating to their work to their Laptop, which is synchronised to a secure school server.
- The school discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside school.
- Staff laptops require a user name and password to be able to access them.
- IEPs, assessment records, pupil medical information and any other data related to pupils or staff is to be password protect prior to a data transference.
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the Senior Leadership Team.

3. Policy Decisions

3.1 Authorising Internet access

All staff must and pupils (for younger children parents will be asked to sign) will read and sign the 'Acceptable Computing Use Agreement' before using any school IT resource.
Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

3.2 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. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.
The school will audit IT provision to establish if the e-safeguarding policy is adequate and that its implementation is effective.

3.3 Handling e-safeguarding 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 head teacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures / safeguarding policy.

4. Communications Policy

4.1 Introducing the E-safeguarding policy to pupils

E-safeguarding rules will be displayed in the IT suite and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.

4.2 Staff and the E-safeguarding Policy

All staff will be given the school E-safeguarding Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

4.3 Enlisting parents' support

Parents' attention will be drawn to the School E-safeguarding Policy in newsletters and on the school Web site.

4.4 Using video conferencing and other online video meetings

All video conferencing activity will be organised, set up and supervised by a suitable member of staff. Pupils will not operate video conferencing equipment. Video conferencing equipment will be switched off and secured when not in use. No video conferencing should be recorded.

5. E-Safeguarding Children

Teachers will ensure e-safety is specifically taught as set out in the National Curriculum 2014 framework. Whole school and Key Stage e-safeguarding assemblies will be conducted at least once a term. Key themes will evolve around preventing children being exposed to the dangers of social media, cyberbullying, personal data protection, messaging and terrorist/extremist material when accessing the internet in line with the Prevent Duty. (also see Computing Policy).

Any E-safeguarding concerns must be reported to the designated safeguarding officer immediately (in accordance with the Safeguarding policy) using the E-Safety concerns sheet 'never do nothing'.