For every child to meet their potential and 'live life in all its fullness.' John 10:10.

E-Safety Policy

Statement of intent

At Hindsford C of E Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives. Whilst we recognise the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material; for example inappropriate images, fake news, racist or radical and extremist views
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

This policy will operate in conjunction with the other important policies in our school, including, but not limited to, our Anti-Bullying Policy, Data Protection Policy, Child Protection and Safeguarding Policy.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Hindsford C of E Primary School's activities.

Legal framework

This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998 (GDPR General Data Protection Act 2018)
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspection Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003

Roles and responsibilities

It is the responsibility of **all staff** to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of the school and to deal with incidents of such as a priority.

The e-safety officer, Mrs Pridding, is responsible for ensuring the day-to-day e-safety in our school and managing any issues that may arise.

The headteacher is responsible for ensuring that the e-safety officer and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

The e-safety officer will provide/organise all relevant training and advice for members of staff on e-safety.

The headteacher will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.

The school will establish a procedure

The e-safety officer will ensure that all members of staff are aware of the procedure for reporting incidents of inappropriate internet use, either by pupils or staff. The e-safety officer will keep a log of all incidents recorded.

Cyber bullying incidents will be reported in accordance with the school's Behaviour policy and Anti-Bullying Policy

The headteacher will hold regular meetings with the e-safety officer to discuss the effectiveness of the e-safety provision, current issues and how to review incident logs, as part of the school's duty of care.

The governing body will then hold regular meetings with the headteacher to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

The governing body will evaluate and review this e-safety Policy on a yearly basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

The headteacher will review and amend this policy with the e-safety officer, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this e-safety Policy.

All staff and pupils will ensure they understand and adhere to our Acceptable Use Policy, which they must sign and return to the headteacher.

Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

Educating Children

'Children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum.'

Keeping Children Safe 2019

Online safety is taught at Hindsford through a variety of channels:

- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Kapow Primary scheme of work. Children build on their learning from the year group before, as seen in out skills progression document
- Key online safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all teaching where opportunities present themselves
- Relevant issues are taught through our Personal, Social, Health and Economic (PSHE) curriculum.

Keeping Children Safe

To keep our pupils as safe as possible:

- in lessons where internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches
- Students will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online.
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- the e-safety officer passes on knowledge of current concerns to be included within learning experiences e.g. new apps or games which may cause concern
- pupils sign an internet use agreement, where they agree to abide by the school rules for internet use. This is detailed in the children's planners.
- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying' and given opportunities to support each other
- Students are instructed to report any suspicious use of the internet and digital devices to their class teacher

- Clear guidance on the rules of internet are displayed around the school

Educating Staff

- All staff will have access to e-safety training and information on an annual basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety.
- All staff will employ methods of good practice and act as role models for students when using the internet and other digital devices.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they have read and fully understand the e-safety Policy.

Filters and Monitoring

- The school works in partnership with Wigan Council, Virtue and Sophos to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-safety officer. If the site was discovered by a pupil, this must be recorded on CPOMS.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Whilst it is essential to ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Internet Access

- Internet access is authorised as staff and students log on and agree to the Acceptable Use Policy**.**
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor students' activity.
- Effective filtering systems will be established to eradicate any potential risks to students through access to particular websites.
- Any requests by staff for websites to be added or removed from the filtering list must be first vetted by the e-safety officer.
- All school systems will be protected by up-to-date anti-virus/malware software.
- Temporary users, e.g. volunteers, must read and sign the school's Acceptable Use Policy

Email

Pupils (if required) and staff will be given approved email accounts and are only able to use these accounts for school business.

- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other students, staff or third parties via email.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources should be deleted without opening them.

Social Networking

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the e-safety officer and head teacher.
- Pupils are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school
- Staff are not permitted to communicate with students over social networking sites except for verified social media accounts e.g. Hindsford's Facebook account.

Published Content

- The headteacher, or nominee, will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the school's websites will be the phone, email and address of the school office
- No personal details of staff or students will be published.
- Images, or any content that may easily identify a student, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Students are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with school's policies in terms of the sharing and distribution of such.

Mobile Devices

- Mobile phones are not permitted to be used by pupils or staff in the classroom.

- In line with our Visitors Policy, any visitors to the building are asked to leave their mobile phone in their vehicle or hand in into the front office for safe keeping. If a visitor is not working directly with the children, and if they need their phone for work purposes, they may be permitted to keep their phone with them, at the school's discretion.
- in school which states that:
- The school accepts that employees will bring their mobile phones to work. It is the responsibility of all staff to sign and follow schools' adherence to safeguarding and child protection policies and our Staff Mobile Phone Policy. Any member of staff found using a mobile phone without permission, or not in line with the school's policies, may be subject to disciplinary action by the Governing Body.

Cyber Bullying

- For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual may experience: Cyber –threats and intimidation, harassment/'cyber-stalking', defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images. (It can include messages intended as jokes, but which have a harmful or upsetting effect.)
- The school will regularly educate staff, students and parents on the importance of staying safe online, as well as being considerate to what they post online.
- The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.
- Any allegations of incidents of bullying will be investigated by our e-Safety Officer, Mrs Pridding. Any incidents of cyberbullying will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

CONDUCT

Incidents of concern should be reported via the school's procedure, as outlined in the safeguarding policy. Written records of concerns are kept detailing incidents. At Hindsford, these records are kept electronically using CPOMS under the e-safety tab.

Misuse by Pupils

- Staff members have the power to discipline students who engage in misbehaviour with regards to internet use, in line with our behaviour policy.
- Any incident deemed serious by a staff member should report it, in line with the school's safeguarding policy.
- Incidents deemed minor should be reported to the e-safety officer, to enable step to be taken to prevent the incident repeating. If the incident involves an individual, this should reported on CPOMS, under the e-safety tag.

- Complaints of a child protection nature shall be dealt with in accordance with our Safeguarding Policy.
- Complaints of a cyber-bullying nature shall be dealt with in accordance with out Anti-Bullying Policy

Misuse by Staff

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher.
- The headteacher will deal with such incidents in accordance with the school's policies, and may decide to take disciplinary action against the member of staff.