Thirsk Community Primary School

Online & Use of Technology Policy

Introduction

Being online is an integral part of children and young people's lives. Social media, online games, websites and apps can be accessed through mobile phones, smart watches, computers, laptops and tablets – all of which form a part of children and young people's online world. The internet and online technology provides new opportunities for young people's learning and growth, but it can also expose them to new types of risks. Online Safety forms a fundamental part of schools' safeguarding and child protection measures. Government guidance for schools across the UK highlights the importance of safeguarding children and young people online. Having a whole school approach helps ensure staff, governors, volunteers and parents teach children about online safety.

Aims

Our aims are to ensure that all pupils, including those with special educational needs, will:

- use the internet and other digital technologies to support, extend and enhance their learning
- develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid inappropriate material
- develop a positive attitude to the internet and develop their ICT skills through both independent and collaborative working
- use existing, as well as up and coming, technologies safely
- demonstrate behaviours which are in line with our school core values and uphold the school rules READY, RESPECTFUL and SAFE**.**

Online Safety Policy Scope

The school Online Safety policy and agreements apply to all pupils, staff, external contractors and members of the wider school community who use, have access to, or maintain school and school-related internet and computer systems internally and externally.

Policy Review Schedule

The policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable internet use policy
- New guidance by Government/LA/safeguarding authorities
- Significant changes in technology used by the schools or pupils in the wider community
- Online Safety incidents in the community, or local schools, which might impact on the school community
- Advice from the police

Monitoring & Evaluation

The Online Safety committee will monitor and evaluate the Online Safety policy. This committee will comprise:

- Head teacher and school leadership team
- Governors
- Designated Safeguarding Lead

In the event of an Online Safety incident, the Designated Safeguarding Lead will differentiate which incidents are required to be reported to CEOP, local police, LADO, Social Care and parents/carers Staff,

parent and pupil Online Safety audits and pupil questionnaires will inform Online Safety learning and staff training requirements.

This will gauge the impact and effectiveness of the Online Safety provision and determine future Online Safety priorities.

We will seek to keep children safe by:

- Ensuring Online Safety is an integrated part of the curriculum
- Specific events and updates such as Safer Internet days, PCSO talks and newsletter updates keep the profile high
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the children using our systems to use the internet, and connected devices in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with children and their parents/carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any learning platforms and new technologies before they are used within the organisation.

How Does Thirsk Community Primary School's Curriculum Provide Online Safety Education?

- Online Safety learning is integrated throughout the computing curriculum
- A dedicated Online Safety unit is taught at the start of each school year.
- Our Computing curriculum content covers the following areas:
- Making safe searches using the internet, keeping personal information safe, SMART rules for internet safety
- What a digital footprint is, using age-appropriate websites, what to do if a website makes them feel uncomfortable, what to do if someone is being unkind online
- Recognise and define cyberbullying, identify safe people to report cyberbullying to;
- Explain what privacy settings are and how to use them safely;
- Explain why it may be dangerous to share private information;
- Identify comments or messages that may be hurtful to others;
- Identify a dangerous spam email;
- Create multiple strong passwords for use across different platform
- Explain what a stereotype is;
- Compare gender stereotypes

If online abuse occurs, we will respond by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- Following the school's Child Protection safeguarding policy, behaviour and anti-bullying policy

- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing policies regularly, in order to ensure that any problems have been resolved in the long term.

E-mail & eSchools

• Pupils and staff will only use approved e-mail and eschools accounts when using the school network
• Pupils will tell a member of staff if they receive inappropriate e-mail or eschools communications
• Pupils will only use e-mail and eschools for approved activities
• eschools is the vehicle by which children and staff communicate online when undertaking distance learning

Internet Access and Online learning platforms

• Staff will read and sign the NYCC Acceptable Use Policy – ICT and Online Safety before using any school ICT resource
• Pupils will read and sign an Acceptable Use Policy
• Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult Mobile Phones / Handheld Technology / Wearable connected devices

Pupils are only permitted to have mobile phones or other personal handheld technology in school with the permission of the Headteacher and they must be handed into the class teacher upon arrival at school and collected after the end of the school day.

Any use during the school day will be under close supervision of a member of staff and permission granted by the Headteacher.

When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's Acceptable Use Policy (AUP). Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others. (Education and Inspections Act 2006, Sections 90, 91 and 94)

Children or staff wearing connected devices must ensure they are not connected the internet during the school day.

If these devices can also be used to take photographs, videos or recordings, they should be treated in the same way as a mobile phone and handed in at the start of the school day. Staff should avoid wearing such devices during the school day.

School Website

All staff who edit or publish web-based content must read and adhere to the Acceptable Use Policy.

Systems Security ICT systems security will be regularly reviewed with support from:
• NYES Digital

Web Filtering The school will work with Schools NYES Digital to ensure that appropriate filtering is in place. The school's filtering is provided by http://www.smoothwall.net/solutions/education/

Pupils will report any inappropriate content accessed to an appropriate member of staff and staff will be vigilant while children are using online devices.

Whole-School Responsibilities for Internet Safety

Headteacher:

- Responsible for Online Safety issues within the school but may delegate the day-to-day responsibility to a Senior Leader or Computing Lead
- Ensure that the Computing Lead is given appropriate time, support and authority to carry out their duties effectively
- Ensure that developments at Local Authority level are communicated to the Computing Lead
- Ensure that the Governing Body is informed of Online Safety issues and policies
- Ensure that appropriate funding is allocated to support Online Safety activities throughout the school

Online Safety/Computing Leader

- Primary responsibility: establish and maintain a safe ICT learning environment (under the direction of Senior Leadership)
- Establish and maintain a school-wide Online Safety programme
- Respond to Online Safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log
- Report to the Senior Leadership Team to review the effectiveness and impact of the policy
- Establish and maintain a staff professional development programme relating to Online Safety
- Develop a parental awareness programme
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area

Governing Body

- The safeguarding governor will ensure that Online Safety is included as part of the regular review of child protection and health and safety policies
- Support the Headteacher and/or designated IT Leader in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment
- Ensure that appropriate funding is authorised for Online Safety solutions, training and other activities as recommended by the Headteacher and/or designated IT Lead (as part of the wider remit of the Governing Body with regards to school budgets)
- Promote Online Safety to parents and provide updates on Online Safety policies

Reviewed November 2022

Date for next review November 2023