Austhorpe Primary School
Online Safety Policy

Date of Policy: September 2025

Online Safety Policy – September 2025

This policy applies to all members of staff, members of the Governing Board and volunteers as well as external agencies using the ICT systems at Austhorpe Primary School.

At Austhorpe Primary School, we seek to develop in our children a love of learning that will last a lifetime. Every child in our school is recognised as individual and unique and it is our aim to help them become the best that they can be in a happy and safe atmosphere with the freedom to engage and discover. Our aim is to create a broad curriculum which develops cultural capital and leads to confident, independent learners, who have a passion for learning and are ready for the next step in their education.

The Austhorpe curriculum is knowledge-rich, taking our pupils beyond their own contexts and supports our commitment for all children to have a deep understanding of the world around them. We recognise the Internet as being an integral part of teaching and learning. The Internet can raise educational standards by offering pupils and teachers opportunities to search for information from a wide range of sources and to enhance the child's knowledge of the outside world. As well as providing many benefits and new opportunities, the use of ICT and the Internet, may lead to safety issues for the children. We accept that this must be managed to protect the children.

To support this, our curriculum includes the *4Cs of online risk of harm*:

- **Content risks**: This may include sexual, violent, inappropriate, biased, false, illegal and prejudicial content.
- **Contact risks**: This includes people who are not known to the child pretending to be someone else such as adults pretending to be children. Or, people who know your children, though they act anonymously to bully and intimidate.
- **Conduct risks**: Behaving in ways that hurt others or victims of such behaviour. Examples are in various games where artificial items can be traded, by tricking or swindling others or deliberately destroying another child's game or digital creation.
- **Contract risks**: This includes children signing up for unfair contracts, terms or conditions that they are not able to comprehend. This could include inadvertently buying in app purchases or subscriptions unwittingly. It could also be accidently setting that allow for private data theft or even fraud.

Online safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks. We know that some adults and children will use these technologies to harm students. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. Staff have a duty of care to protect children from risk of harm, as well as a duty to ensure their own conduct does not bring into question their suitability to work with children.

This guidance considers the principles of the Safer Working Practice Guidance (National Safer Recruitment Consortium) as well as guidance from the Department for Education (Safeguarding Children in a Digital World), CEOP (Child Exploitation and Online Protection) and Communication Act 2003 (Section 127 Improper Use of Public Electronic Communications Network). http://www.legislation.gov.uk/ukpga/2003/21/section/127

At Austhorpe, we aim to:

- Educate children to help them to develop a safe, responsible and mature attitude towards Internet use, inside and outside the school environment,
  Regulate Internet access to ensure children are using websites and materials that are appropriate to them,
  All staff to monitor children's access to the Internet both in school and at home
- Establish home school agreements, involving parents and children and staff about acceptable use of the Internet, including school 1:1 devices that are taken off-site.
- Ensure that all staff and pupils regularly revisit online safety learning and maintain this as a specific focus for Health and Well-being Week and Anti-Bully Week

Internet use will support, extend and enhance learning:

- Children will be given clear objectives for Internet use,
- Web content will be subject to age-appropriate filters,
- Internet use will be embedded in the curriculum.

Children will develop an understanding of the uses, importance and limitations of the Online Safety Policy:

- Children will be taught how to effectively use the Internet for research purposes,
- Children will be taught to evaluate information on the Internet,
- Children will be taught how to report inappropriate web content through the use of the CEOP button.

Children will develop a positive attitude to the Internet and develop their ICT capability through both independent and collaborative working:

- Children will use the Internet to enhance their learning experience,
- Children have opportunities to engage in independent and collaborative learning using the Internet and other digital technologies.

Roles and responsibilities:

Governing Board and Red Kite Learning Trust

The governing board is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online

safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the SLT in regard to training, identified risks and any incidents.

Headteacher:

Reporting to the governing board, the Headteacher has overall responsibility for e-safety within our school. The Headteacher will ensure that:

Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. children, all staff, governing body and parents.
All online safety incidents are dealt with promptly and appropriately.

Online Safety Leader:

The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst being familiar with the latest research and available resources for school and home use.
- Review this policy regularly.
- Advise the governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the Red Kite Learning Trust IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log on CPOMS; ensure staff know what to report and ensure the appropriate audit trail.

School staff and volunteers:

- Staff are responsible for their own actions and must act, and be seen to act, in the best interests of children at all times.
- Staff must ensure they understand and adhere to this guidance as well as Austhorpe Primary School's Acceptable Use Policy.
- Staff are responsible for acting promptly to prevent and safeguard children from potential abuse online and for reporting any concerns in accordance with the Leeds Children's Services Safeguarding & Child Protection Policy for Schools and Colleges.

ICT Technical Support Staff Technical support staff (RKLT Help Desk) are responsible for ensuring that:

- The IT technical infrastructure is secure.
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices
- Windows (or other operating system) updates are regularly monitored, and devices updated as appropriate.
- Any online safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer/Headteacher.
- Passwords are applied correctly to all users regardless of age
- Any inappropriate websites are blocked from use and that filters are up-to-date and effective – follow up is timely and alerts RKLT helpdesk

All users:

All users are to ensure that:

All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher.

Any online incident is reported to a member of the Safeguarding team via typical communication methods and logged on CPOMS.

All Children:

- The Acceptable Use Policy applies to all ICT equipment and services in this school, any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- Online Safety is embedded into our curriculum; children will be given the appropriate advice and guidance by staff. Similarly, all children will be fully aware how they can report areas of concern whilst at school or outside of school.
- Understand that any improper use of IT equipment, their IT accounts or the internet will result in their accounts being suspended while school staff investigate any concerns
- Will sign the Acceptable Use agreement for access to online learning, use of IT equipment and accounts and also mobile phone use.

Parents and Carers:

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge, they need to ensure the safety of children outside the school environment. Through parents' evenings and school newsletters, the school will keep parents up to date with new and emerging online safety risks and will involve parents in strategies to ensure that children are empowered. Parents/ carers must also understand the school must have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the children's Acceptable Use Policy before any access can be granted to school ICT equipment or services. They will understand that in response to any cyber-bullying incident, school will react in a

reasonable, proportionate and consistent manner whether this is within the school day or outside of school hours.

1:1 iPad Scheme:

- All children and their parents/carers, who are enrolled in the 1:1 iPad scheme, will read and agree to the relevant Acceptable Use Policy.
- Children and parents who do not agree to our Acceptable Use Police will not be permitted to take their iPads home.
- All iPads will have RKLT management software installed and have filtering enabled within school.
- As part of the Acceptable Use Policy, Austhorpe Primary School has the right to monitor usage of iPads to ensure that users are adhering to the Acceptable Use Policies; this is completed half termly.
- Monitoring of 1:1 iPads will take place half-termly on a selection of devices. All devices will be check at least twice, during each academic year.

AI

All staff are expected to use AI in accordance with the Trust AI Policy and the systems established by the Trust. Before using any AI system, staff must:

- consult the AI Register
- confirm that the AI tool is listed and approved for the intended use
- familiarise themselves with the permitted uses and any restrictions recorded in the AI Register
- report any misuse, unauthorised access or data protection concerns promptly

In terms of expected professional standards and behaviours, staff are expected to:

- attend training provided by the Trust
- understand that AI is a support tool designed to enhance teaching and delivery but is never a substitute for professional judgement.
- understand that the quality and content of any final material(s) remains their responsibility.
- remain responsible and accountable for the accuracy, appropriateness and quality of any AI-generated material they use or adapt, including in contexts such as:
    - creating or adapting educational resources
    - planning lessons or curriculum content
    - drafting tailored feedback or revision materials
    - supporting administrative tasks such as report writing or meeting preparation

Staff must not use AI systems:

- to make decisions that carry significant consequences for pupils or staff (e.g. safeguarding, behaviour, performance, SEND)
- to assess subjective work without applying their own professional judgment
- to impersonate others or present AI-generated work as wholly human-authored
- for any purpose that is unlawful, misleading or outside the scope of approved use

Staff are expected to uphold all relevant legal and regulatory standards when using AI, including:

- data protection and UK GDPR
- copyright and intellectual property rights
- equality legislation
- duties under Keeping Children Safe in Education

Prevent:

In order to fulfil our Prevent duty, it is essential that staff can identify children who may be vulnerable to radicalisation, and know what to do when they are identified. Protecting children from the risk of radicalisation is seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other harms (e.g. drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences. For further information, refer to Safeguarding and Child Protection Policy and the Preventative Curriculum Programme for Child on Child Abuse.

Anti-bullying Policy

For further information about the school response to cyber-bullying or concerns linked to online materials, sites or communication tools, please see our Anti-Bullying Policy as support.

GDPR

All school devices, and the data of users held on such devices, are operated under the school's Data Protection Policy. This policy also applies to devices that are used as part of the school's 1:1 iPad scheme.