Online (E)-Safety Policy

Date of review: June 2025

Date of next review: June 2026

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Cyber-bullying: advice for headteachers and school staff

It also refers to the DfE's guidance on protecting children from radicalisation.

This policy should be read in association with:

- The Acer Trust Cyber Security Policy
- The Acer Trust Social media for Staff Policy
- The Acer Trust Data Protection and Freedom of Information Policies
- The School Behaviour, Anti-bullying and child protection and safeguarding policy
- The Acer Trust Acceptable Use Agreements for staff, students, volunteers and governors
- The Acer Trust Staff Code of Conduct
- The Acer Trust Pupil/staff privacy notices.
- The School Laptop loan policy

It has been agreed and approved by the Governing Body and will be reviewed annually.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running theme through the school approach to safeguarding
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children.

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy, are appropriately trained and that it is being implemented consistently throughout the school
- Working with the headteacher and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety or cyber-bullying incidents are dealt with appropriately in line with this policy
- Liaising with other agencies and/or external services if necessary

3.4 The SBM/IT Support

The SBM with guidance from the IT Support contract is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems
- Ensuring that the school's ICT systems are secure and protected against viruses and malware
- Locking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents or cyber-bullying are dealt with appropriately in line with this policy

3.5 All staff

All staff are responsible for:

- Understanding and implementing this policy consistently
- Participating in appropriate training and having an up-to-date awareness of online safety matters. They are kept up-to-date with information through staff INSET, guidance information and selfstudy.
- Agreeing and adhering to the terms of acceptable use of the school's ICT systems and the internet, social media, cyber security and staff code of conduct
- Ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety or cyber-bullying incidents are dealt with appropriately in line with this policy
- Reporting any suspected misuse, by pupil or adult, to the headteacher, School Business Manager or DSL as soon as possible
- Ensuring that any online communication with pupils or parents is professional
- Ensuring that online safety is planned for and embedded into their teaching
- Monitoring the use of digital technologies, mobile devices, cameras etc by pupils and adults and implement policies where applicable

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (found on the school website)

3.7 Visitors, Volunteers and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Teaching and learning

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils to raise educational standards, promote pupil achievement and to support the professional work of staff. It is an essential element in 21st century life for education, business, and social interaction. The school therefore has a duty to provide students with quality Internet access as part of their learning experience.

Through our computing, SRE and wider subject curriculum, our pupils are taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and behaviour in an age-appropriate way that is relevant to their pupils' lives.

Full details of the E-safety teaching and learning can be found on the school website under the E-safety progression of skills document. To summarise:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online even when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, by sharing this policy and via the curriculum information available on the school website.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

6. Acceptable use of school internet including email and social media

For School Purposes

All pupils, staff, volunteers and governors are expected to read and adopt an agreement regarding the acceptable use of the school's ICT systems and the internet. Staff are also expected to adhere to the requirements laid out in the Staff Code of Conduct and the Social medial policy.

These documents clarify that the use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Websites visited by pupils, staff, volunteers, governors and visitors (where relevant) will be monitored to ensure they comply. Some social networking sites and news groups are blocked unless a specific use is approved.

Additionally, pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They also must acknowledge the source of information used and respect copyright when using Internet material in their own work.

The School ensures that the use of Internet-derived materials by staff and by pupils complies with copyright law.

For Personal Purposes

In terms of good practice for personal use of the internet, pupils are advised:

- Never to give out personal details of any kind which may identify them or their location.
- Not to place personal photos on any social network space.
- Not to sign up to any social networking site that is not age-appropriate. eg. Facebook
- To consider security by setting passwords, denying access to unknown individuals and are instructed how to block unwanted communications.

Pupils do not currently use the Internet in school for emailing as individuals and do not have an email account.

Staff will adhere to the Social media guidance for staff laid out in Appendix 1 of the Social media policy. This includes not running social network spaces for students on a personal basis or being in contact with parents from the school on social network sites

Staff are advised to use their school email addresses for any school related correspondence but to be aware that this is not a secure system. Passwords should be considered for documents that contain sensitive information.

7. The School website and social media presence

The headteacher has overall editorial responsibility to ensure that content of the school website and facebook page is accurate and appropriate. The contact details on these platforms are the school's address, office e-mail, and telephone number. Other email addresses are generally not published, to avoid spam harvesting.

Parents or carers are regularly asked via an online permission form if the school can use their child's photograph in school publications (which includes the school website and social media). Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified by name. Images of staff are not published without consent from that member of staff. Pupils' full names are not used anywhere on social media, particularly in association with photographs.

8. Staff using work devices outside school

All staff members taking school devices offsite will take appropriate steps to ensure their devices remain secure. They will work in line with the requirements of the laptop loan, cyber security and data protection policy. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

9.Internet Access, cyber security and data protection

In line with our cyber security and data protection policy, our third party IT support contract uses content filtering to protect pupils from accessing inappropriate internet content. The

headteacher, IT Technician and School Business Manager ensure that the filtering methods selected are appropriate, effective, and reasonable.

Additionally, fire walls and virus/malware protection are installed and updated regularly to protect our systems, with offsite back-ups of data held on school servers. Servers and other hardware are located in secure areas with access restricted to appropriate staff.

Levels of internet access and supervision are decided as appropriate to the user and supported through the management of network accounts and passwords. Staff access to personal, private or sensitive data and information is restricted to authorised users only, with procedures being followed for authorising and protecting login and password information.

In class, pupils learn about safe practice regarding use of their login details, including passwords.

If staff or pupils discover unsuitable sites, the URL, time, date and content must be reported to the Internet Service Provider/IT Support via the headteacher. Any material that the school believes is illegal is reported to appropriate agencies such as:

- Internet Watch Foundation (IWF) : www.iwf.org.uk
- Child Exploitation and Online Protection Centre (CEOP) : www.ceop.police.uk
- If appropriate, the Local Authority Designated Officer for Safeguarding (LADO)

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, including any alleged incidences of cyber bullying, we will follow the procedures set out in our behaviour and anti-bullying policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedure. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, and staff meetings).

12. Monitoring arrangements

This policy will be reviewed every year. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.