THRUNSCOE PRIMARY AND NURSERY ACADEMY

E-SAFETY POLICY

Rationale

As a Community Academy working with our local, national and international communities, ICT in the 21st Century is seen as an essential resource to support and enhance learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, academies need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- Virtual reality headsets
- Artificial Intelligence- pupils must not use generative AI tools (e.g., OpenAI, ChatGPT, or similar platforms) for any academy-related work.

Whilst exciting and beneficial, both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Thrunscoe Primary and Nursery Academy, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors, parents and pupils) are inclusive of both fixed and mobile internet; technologies provided by the academy (such as the new computer suite, laptops, IPad's, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto the academy premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the academy the Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Head teacher. Any extra permission given by the Head must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The named person (Safeguarding Officer) and Computing Coordinator have the responsibility of ensuring this policy is upheld by all members of the academy community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as the LA, Becta, CEOP (Child Exploitation and Online Protection), Childnet and Local Authority Safeguarding Children Board.

This policy, supported by the academy's acceptable use agreements for staff, governors, visitors, parents and pupils, is to protect the interests and safety of the whole academy community. It is linked to the following mandatory academy policies: child protection, health and safety, home–academy agreements, safeguarding policy and behaviour (including the anti-bullying) policy.

E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues in the form of full staff meetings and notices at regular staff meetings.
- New staff receive information on the academy's acceptable use policy as part of their induction through their staff handbooks.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the academy community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Communicating the academy e-safety messages

- E-safety rules will be posted on the laptop trollies and discussed with the pupils at the start of each year.
- Pupils are informed that network and internet use is monitored within the academy.
- The pupil council will discuss e-safety within the academy, to raise the profile.

E-Safety in the Curriculum

- ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety. We actively monitor and assess our pupils' understanding of e-safety.
- The academy provides opportunities within a range of curriculum areas and discrete ICT and PSHE lessons to teach about e-safety (in accordance with the medium term planning).
- The first ICT lesson each academic year (in all year groups) is to be focused on e-safety and is provided through Kapow computing curriculum.
- Educating pupils on the dangers of technologies that may be encountered outside of the academy may also be done informally when opportunities arise.
- Pupils are made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline/ CEOP and report abuse button.
- Internet safety awareness sessions take place within the academy for children, parents and the wider academy community, generally on or around Safer Internet Day and evidence of this is collected by the Computing coordinator.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.
- When teaching about Artificial Intelligence, staff must ensure pupils understand safe, ethical, and age-appropriate use, and that generative AI tools are not to be accessed independently.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data.

All pupils have separate logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security; however, pupils cannot reset their own passwords.

Laptops are pre-programmed to initiate password updates on a regular basis, to minimise security risks.

Data Security

The accessing and appropriate use of academy data is something that the academy takes very seriously. Staff are aware of their responsibility when

accessing academy data. Level of access is determined by the Head Teacher. All teaching staff have been granted home access to the shared network via a VPN. Any memory sticks used by staff to transport date must be encrypted. All teacher laptops and teacher iPads have been password protected. Staff must not input any pupil data into external AI platforms.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up by the Computing Coordinator and/or the ICT technician (depending on the circumstance).

- All staff, parents, pupils and visitors must read and agree to the 'Acceptable ICT Use Agreement' before using any academy ICT resource.
- In the Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with some access to specific, approved on-line materials.
- Staff will always preview any recommended sites before use.
- Unchecked image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- The Academy homepage consists of safe search engines that the children must use in the academy. Parents are advised to access this homepage before their children search the internet.
- All users must observe software copyright at all times. It is illegal to copy or distribute academy software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Academy internet access is controlled through the Central I.C.T's web filtering service.
- Staff and pupils are aware that academy based email and internet activity is monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the class teacher who must inform the Computing co-ordinator or I.C.T. technician.
- It is the responsibility of the academy, by delegation to the technical support; to ensure that Anti-virus protection is installed and kept up-to-date on all academy machines.
- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.

- Pupils and staff are not permitted to download programs or files on academy based technologies without seeking prior permission from the I.C.T. technician, computing coordinator or business manager.
- If there are any issues related to viruses or anti-virus software, the Computing Coordinator, I.T. Technician and Office staff should be informed through the 'Computer Problems' book held in the staff room (on I.C.T. technician's desk).

Managing Social Media and Networking Sites

- At present, the academy denies access to social media and networking sites such as Facebook to pupils and staff.
- There should be no communication between staff and pupils through social media and networking sites such as Facebook.
- Parents are requested not to post photos/videos taken in or on the Academy grounds on social media and networking sites.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, academy details, email address, specific hobbies/interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the academy.
- Parents are reminded of the strategies their children are taught during yearly e-safety information letters.
- Parental/ guardian is sought before putting images/videos of pupils on the academy website/social media platform (refer to- safe use of image subheading).

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in the academy is allowed. Our academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones):

- The academy allows staff to bring in personal mobile phones and devices for their own use. Mobiles must be kept in the teacher's bags or in a cupboard and only used during non-contact time with pupils. Phones should not be in use during times when staff should undertaking paid roles as per their contract, unless with prior agreement from the Head Teacher.
- Staff are strongly advised not to contact a pupil or parent/ carer using their personal device.
- Older pupils who walk to and from the academy are permitted to bring personal mobile phones to the academy but such devices must be handed to a class teacher at the start of the day, switched off and not used within the grounds of the academy.
- If such a device is heard or seen during the academy day, it will be confiscated and a responsible adult will be required to claim it from the head teacher. In such circumstances the head teacher will give a reminder about e-safety.
- The phone remains the responsibility of the child at all times and no responsibility is accepted by the academy for the loss, damage or theft of any personal mobile device.
- Users bringing personal devices into the academy must ensure there is no inappropriate or illegal content on the device.

Managing email

The use of email is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including; direct written contact between academies on different projects, be they staff based or pupil based, within the academy or internationally. We recognise that pupils need to understand how to style an email in relation to their age and good 'etiquette'. As part of the Purple Mash computing, pupils must have experienced sending and receiving emails.

- The academy gives all staff their own email (xxxxx@thrunscoe.academy) account to use for all academy business.
- Children will email using the academy email system (Purple Mash). This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff are never to give personal email addresses to pupils
- Under no circumstances should staff contact pupils, parents or conduct any academy business using personal email addresses.
- E-mails sent to an external organisation should be typed carefully and should contain a full email signature before sending, in the same way as a letter written on academy headed paper.
- Pupils may only use academy approved accounts on the academy system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in our academy. Pupils may forward any chain letters causing them anxiety to the Computing coordinators e-mail account. The head teacher will be informed, when necessary.

- All e-mail users are expected to adhere to the generally accepted rules of network etiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Staff must inform the Computing coordinator and/or Head teacher if they receive an offensive e-mail.

Safe Use of Images - Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the academy community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the academy permits the appropriate taking of images by staff and pupils with academy equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on academy visits.
- Pupils are permitted to use equipment, including iPods and cameras, to record images of others; this includes when on academy visits. These photos and videos remain inside the academy and are only published onto the website if permission has been gained from parents. However, in some circumstances (academy residential's) photos may be kept for personal collection.

Publishing pupil's images and work

On a child's entry to the academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

  - on the academy web site
  - in the academy prospectus and other printed publications that the academy may produce for promotional purposes
  - recorded/transmitted on a video or webcam
  - general media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
  - Social media.
- This consent form is considered valid for the entire period that the child attends this academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
- Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by one parent/carer
- Pupils' full names will never be published alongside their image and vice versa.

- E-mail and postal addresses of pupils will not be published.
- Pupils' work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

- Images/films of children are to be stored in the 'photos' folder or the 'Class Teachers' folder within the staff area of the server. They should be removed when they are no longer needed.
- Images shown on other areas of the academy's network must be temporary in nature and removed as soon as possible.
- Images taken on portable media (Cameras, teacher iPads etc must be deleted as soon as they have been uploaded so that the media is 'empty'
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the academy network/Learning Platform.
- Teaching Staff have the responsibility of deleting the images when they are no longer required.

Misuse and Infringements

Complaints:

- Complaints relating to e-safety should be made to the Head Teacher.
- All incidents will be logged and followed up.
- Complaints of a child protection nature must be dealt with in accordance with academy child protection procedures and must be reported to the Child Protection Officer (Head teacher) or in their absence, The Deputy Child Protection Officers (Miss J Howden Deputy Head teacher /Mrs K. Allen Well-Being Mentor)
- Pupils and parents will be informed of the complaints procedure.

Inappropriate material (see ICT Acceptable Use Agreement):

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head Teacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the head teacher, removal of the right to access ICT within the academy (pupils) and depending on the seriousness of the offence may lead to an investigation by the Head Teacher/LA, and for staff, could involve immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Equal Opportunities: Pupils with additional needs

- The academy endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the academy's e-safety rules.
- However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of the academy. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits related to Computing and associated risks.

Parents/carers are asked to read through and sign acceptable use agreements on admission of their child to the Academy.

Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on the academy website)

The academy disseminates information to parents relating to e-safety where appropriate in the form of;

- Information sessions
- Posters
- Newsletter/email items

Parents will be advised that the use of social network spaces is inappropriate for primary aged pupil.

Parents/carers are expected to reinforce the guidance from the academy when using technologies at home. The academy will not be responsible for communications between pupils' outside the academy through social networking sites/ platforms or for pupils accessing inappropriate sites outside of the academy.

ICT Acceptable Use Agreement (AUA)

POLICY STATEMENT

The Governing Body recognises the use of ICT as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for Computing to enhance development in all areas of the curriculum and academy administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities,

especially for ensuring that children are protected from contact with inappropriate materials.

In addition to their normal access to the academy's Computing systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and e-mail and internet facilities during their own time subject to such use: not depriving pupils of the use of the equipment and/or not interfering with the proper performance of the staff member's duties. Whilst the academy's ICT systems may be used for both work-related and for personal reasons the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times and must never compromise the high standards of Safeguarding expected by all members of the staff.

The use of computer equipment, including laptop computers, which is on loan to staff by the academy for their personal use at home is covered under this policy. Staff who have equipment on loan are responsible for its safekeeping and for ensuring that it is used in compliance with this policy.

GUIDANCE ON THE USE OF ACADEMY ICT FACILITIES

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any non-conformance to this policy or operation outside statutory legal compliance may be grounds for disciplinary action being taken up to and including disciplinary action
Further guidance on the responsible use of ICT facilities are contained in the Thrunscoe Primary Academy document "Internet Access Policy".

E-mail and Internet usage
The following uses of the academy's ICT system are prohibited and may in certain circumstances amount to gross misconduct and could result in dismissal:

1. to gain access to, and/or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it
2. to gain access to, and/or for the publication and distribution of material promoting racial hatred
3. for the purpose of bullying or harassment, or for/in connection with discrimination or denigration on the grounds of gender, race, disability or sexual orientation
4. for the publication and/or distribution of libellous statements or material which defames or degrades others
5. for the publication and distribution of personal data without either consent or justification
6. where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination

7. to participate in on-line gambling
8. where the use infringes copyright law
9. to gain unauthorised access to internal or external computer systems (commonly known as hacking)
10. to enable or assist others to breach the Governors' expectations as set out in this policy

Additionally, the following uses of academy ICT facilities are not permitted and could lead to disciplinary action being taken:

1. for participation in "chain" e-mail correspondence
2. in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade union representatives)
3. to access ICT facilities using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.

Use of Academy ICT Equipment

Users of Academy ICT equipment:

1. must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries
2. must report any known breach of password confidentiality to the Head teacher or Computing Co-ordinator as soon as possible
3. must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the academy's ICT systems
4. must not install software on the academy's ICT systems, including freeware and shareware, unless authorised by the academy's Computing Co-ordinator/ICT Technician
5. must comply with any ICT security procedures governing the use of systems in the academy, including anti-virus measures

Please sign the staff sheet to acknowledge that you have read and understood the ICT and e-safety policy and guidelines.

AUP's must also be signed by all Staff, Visitors, Parents and Children with access to the academy ICT network and ICT equipment. Signed copies are held centrally within the academy office.

Policy reviewed: March 2026 by Mr A. Howard

Approved by the Governing Body on: Thursday 19th March 2026

Next review date: March 2028