

E-Safety (Online Safety) Policy

Auckley Primary Academy

Reviewed & Updated December 2025

This policy applies to all members of the school community — pupils, staff, governors, visitors, volunteers, and contractors — and includes the Acceptable Use Agreements for adults and pupils.

1. Introduction

Digital technologies are an essential part of teaching, learning and daily life. They include, but are not limited to:

- Websites and web tools
- Coding and online learning platforms
- Gaming, apps and social networking
- Mobile devices (phones, tablets)
- Video and multimedia services

All users should understand the benefits and risks associated with these technologies. The school has a duty to educate pupils about online safety and related behaviours, including how to manage risks, harmful content and online relationships.

This policy links directly to the school's safeguarding procedures, and it sits alongside other related policies including *Child Protection*, *Data Protection (GDPR)*, *Behaviour* and *Bullying*.

2. Legal and Statutory Context

This policy follows statutory safeguarding guidance outlined in *Keeping Children Safe in Education* (KCSIE). Schools must ensure appropriate filtering and monitoring arrangements are in place and regularly reviewed. [UK Safer Internet Centre](#)

It also reflects guidance from the UK Safer Internet Centre's online safety policy templates and requires regular updates as technology and legal expectations change. [UK Safer Internet Centre](#)

The policy covers all online activity carried out on school devices, school networks, during remote learning, and where pupils represent the school online.

3. Roles and Responsibilities

Headteacher and Governors

- Ensure the e-safety policy is implemented and reviewed annually.
- Ensure adequate training, resources and monitoring are in place.

Designated Safeguarding Lead (DSL)

- Leads on online safety and liaises with staff, IT support and governors.
- Monitors risks and reports incidents appropriately.

IT Support

- Ensure security measures (firewall, filtering, monitoring) function effectively.
- Support staff and SLT through reporting and technical response.

All Staff

- Implement the policy and report e-safety concerns.
- Educate pupils about online risks and safe behaviours.

Pupils and Parents/Carers

- Sign up to the Online Safety Agreements and follow the rules.
 - Support safe behaviours on school and home devices.
-

4. E-Safety Education and Curriculum

E-safety is embedded across the computing curriculum and reinforced through:

- Direct lessons on online risks (bullying, harmful content, privacy, relationships).
- Behaviour and PSHE lessons supporting positive digital citizenship.
- Guidance on reporting concerns (trusted adult, reporting buttons, CEOP). [NSPCC Learning](#)

Pupils are taught to:

- identify online risks and report concerns
- understand age-appropriate use of apps and online platforms
- engage respectfully and responsibly in digital spaces

We follow the DARES curriculum which includes digital literacy lessons throughout the year. (please see concept map on curriculum page of the website)

5. Acceptable Use Agreements

All users must abide by the Acceptable Use Agreements:

Staff, Governors & Visitors:

- Use school IT and email systems only for professional purposes.
- Protect passwords, data, and pupil information.
- Only use approved software and devices.
- Report misuse or incidents immediately.
- Only use school equipment to take/record images of pupils.

Pupils:

- Use devices and the internet responsibly and politely.
- Keep personal information private.
- Follow rules for online interaction and report concerns.

Agreements are part of induction and are re-signed annually.

6. Internet Use, Filtering, Monitoring and Security

The school's internet is filtered and monitored to help protect users and comply with statutory obligations. [UK Safer Internet Centre](#)

- Filtering systems aim to block harmful content while allowing appropriate educational access.
- Monitoring tools help identify potentially risky behaviours.
- Reports of inappropriate access or behaviour are investigated under school procedures.

Users must not attempt to bypass filtering or monitoring systems.

7. Data Protection and Confidentiality

All processing of personal data complies with UK GDPR and the Data Protection Act 2018.

- Staff use encrypted, password-protected devices provided by school.
 - Data is stored securely on the school server.
 - Personal data must not be stored on removable devices without authorisation.
-

8. Remote Learning and Meetings

We use Microsoft Teams for remote learning and virtual meetings. When using Teams:

- Staff must ensure backgrounds, clothing and surroundings are appropriate.
- Cameras should focus on staff only; minimise distractions.

- Confidential information must not be visible.
 - Staff should end meetings properly to ensure pupils cannot remain online unsupervised.
 - Pupils must follow behaviour expectations as they would in school. [GOV.UK](https://www.gov.uk)
-

9. Mobile Phones and Personal Devices

- Pupils may bring phones only if essential (e.g. walking home independently).
 - Phones must be switched off and stored securely during school hours.
 - Staff may bring personal devices for use outside classrooms but must not use them with pupils or to record images.
 - Guest Wi-Fi access is separate from school networks.
-

10. Social Media and Online Platforms

- Pupils are not permitted to access personal social or gaming accounts on school devices or networks.
 - Staff must not communicate with pupils through personal social accounts.
 - School social media accounts must be managed professionally with consent permissions for the use of pupils' images.
 - Adults should ensure their personal online profiles do not conflict with their professional role.
-

11. Use of Images and Publishing Work

- Images of pupils are only taken with *written consent* from parents/carers.
 - Pupils' names should not accompany photographs on public platforms.
 - All published work/images must comply with data protection and consents.
-

12. Reporting, Misuse and Sanctions

- All users should report accidental access to inappropriate content.
- Deliberate misuse is investigated by leadership and sanctions applied where appropriate.
- Incidents may be recorded and shared with parents/carers.

Complaints follow the school's established procedures.

13. Supporting Pupils with Additional Needs

We recognise that some pupils may require extra support to understand e-safety concepts. Staff provide differentiated guidance, reminders, and scaffolding where needed.

14. Review and Policy Updates

This policy is reviewed at least annually or when major legal or technical changes occur (e.g., new statutory guidance, Online Safety Act implementation through Ofcom, updated filtering/monitoring standards). [Glide](#)

Key Supporting Links (included in policy)

Online Safety Policy Guidance — UK Safer Internet Centre:

<https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/online-safety-policy> UK Safer Internet Centre

Filtering and Monitoring Expectations (DfE via UK Safer Internet Centre):

<https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring> UK Safer Internet Centre

Safeguarding and Remote Learning (DfE):

<https://www.gov.uk/guidance/safeguarding-and-remote-education> GOV.UK

Online Safety & Schools — NSPCC Learning:

<https://learning.nspcc.org.uk/online-safety/online-safety-for-schools> NSPCC Learning

Auckley Primary Academy

Staff, Governor and Visitor Acceptable Use Agreement (Visitors who are accessing IT equipment in school)

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All users are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the SLT.

- I will only use the school's email / Internet / Website and any related technologies for professional purposes.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school related activities.
- I will ensure that personal data is kept secure and is used appropriately. Laptops are encrypted but must be kept secure if taking home.
- I will not install any hardware or software on school equipment without the permission of the Trust IT Technician.
- I will not allow anyone external to the school to use a memory stick in my school computer.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with data protection policy and the safer use of images policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher in line with data security policy. Only school equipment may be used to record and photograph pupils.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Head Teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

Remote Technology Protocol:

When delivering remote education online the same principles set out in the staff Code of Conduct will apply.

- **Staff should have in mind their safeguarding obligations and should report any safeguarding concerns according to the school policy.**
- All staff should wear appropriate clothing, the background should be neutral and desk/ table should be clear.
- Other household members should not be seen on the screen, and whilst online you should not be interrupted.
- Microphones should be muted when the input is finished so that incidental conversations cannot be heard.

- Staff can move away from the computer once lesson input has been given to allow children to work independently. If this is done, ensure that you click the red leave button, then end meeting.
- Staff should remain professional at all times.
- Make sure that any other tabs that are open in the browser are appropriate for a child to see if you are sharing a screen.
- Decide if you are going to disable chat as this can be a distraction to learning.
- Always use **'End Meeting' on the red button** to ensure that no children remain on TEAMS unsupervised.
- If you click the three dots, you can use **spotlight** for yourself so that only you can be seen and rest of children cannot be seen by others. Click **focus**, so that your presentation is the main item on the screen.
- Always take a register for each session and ask child to turn camera on for this.
- Record any incidents or issues as well as informing SLT.
- Do not allow anyone on a teaching session who is not using the child's log in.
- Use teams to schedule meetings and ensure that you don't allow others to bypass the lobby. This means that the session cannot start without you.

The children should be taught the following to enable the sessions to run smoothly:

- How to mute and use the hand symbol. The expectation is that they are on mute, unless told otherwise.
- How to turn their camera off, if required.
- They should be dressed appropriately and have the resources they need to hand.
- The children should be in a quiet place, free from interruptions with an appropriate background behind them. This space should be a shared space in their house.
- Classroom standard of behaviour is expected from all participants.

User Signature

I agree to follow this Acceptable Use Agreement and abide by the E-safety policy

Signature Date

Full Name (printed)

Please return signed copy to Admin.

Auckley Primary Academy

Pupil E-Safety Agreement

When I am working on a computer or device in school or at home:

- I will only use the computer in school for school purposes.
- I will only use my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- I will make sure that all computer related contact with other children and adults is appropriate and polite.
- I will not deliberately look for, save or send anything that could offend or upset others.
- If I accidentally find anything inappropriate on the internet, I will tell my teacher or a trusted adult immediately.
- I will not give out my personal details such as my name, phone number, home address or school.

- I will be responsible for my behaviour when using computers in school or at home because I know that these rules are to keep me safe.
- I will not arrange to meet someone who I have met online, or give them information about me or share photographs. I will tell a trusted adult if I am contacted by someone I don't know.
- I know that my use of computers can be checked and that my parent or carer contacted if a member of school staff is concerned about my safety.



Children's Remote Learning Agreement. (Microsoft Teams)

1. I need to sit in a shared space in my house, where a parent/ carer is available if needed. This space should be quiet and free from interruptions.
2. I need to be dressed appropriately and I should have everything I need for the lesson ready, e.g. paper, pens, work booklet.
3. I will behave appropriately, as I would if I was in the classroom at school.
4. My teacher will tell me how to use the hand tool and I will use this sensibly if I need to.

5. I will mute my microphone if told, and leave it muted unless told otherwise.
6. I will not record the session.
7. I will not use the chat box unless directed to by the teacher and I will be sensible when using it.
8. If requested, I will turn my camera off, and not turn it on unless told to, so that I can concentrate on the teacher and the screen.
9. My teacher will tell me how long the session will last and give me instructions about what to do. I will follow these carefully.

This has been shared with your child today in preparation for any future computer work at home and at school.