Huish Episcopi Academy

The best in everyone™

Part of United Learning

E-Safety Policy

Background

The internet and other digital technologies are powerful tools that provide new opportunities for learning and communication. Used appropriately, they can:

- Stimulate discussion
- Promote creativity
- Increase awareness of context
- Support effective teaching and learning
- Children and young people are entitled to safe internet access at all times.

E-safety is part of the wider duty of care owed by all Academy staff. This policy is designed to ensure safe, appropriate use of technology and has been developed with input from governors, senior leaders, staff, parents, students, and the wider community.

While digital tools raise educational standards and promote achievement, they also present risks, including:

- Exposure to illegal, harmful, or inappropriate content
- Unauthorised access to, loss, or sharing of personal information
- Online grooming
- Sharing or distribution of personal images without consent
- Inappropriate communication with strangers
- Cyberbullying
- Access to unsuitable games or media
- Inability to evaluate online information critically
- Plagiarism and copyright infringement
- Illegal downloading of files
- Excessive use impacting wellbeing

As with offline risks, these cannot be completely eliminated. Instead, our role is to build resilience so that students have the confidence and skills to recognise and respond to challenges online.

Scope of the Policy

This policy applies to all members of the Academy community, including:

- Staff
- Students
- Volunteers
- Parents/carers
- Visitors
- Community users

It applies both in and outside the Academy where individuals use the Academy's ICT systems or represent the Academy.

The **Education and Inspections Act 2006** gives Headteachers authority to regulate students' behaviour outside school where it relates to Academy membership. This includes cyberbullying and other e-safety incidents beyond the Academy site.

Roles and Responsibilities

Governors

- Approve and review the E-Safety Policy.
- Receive regular reports from the Designated Safeguarding Lead (DSL).

Principal/Senior Leaders

- Ensure the safety of the Academy community.
- Delegate day-to-day e-safety responsibilities to the DSL.
- Establish procedures for handling serious e-safety allegations against staff.

DSL E-Safety Lead

- Lead on developing and reviewing e-safety policies.
- Provide training and guidance to staff.
- Liaise with ICT staff and external agencies where necessary.
- Keep a log of incidents and report regularly to governors.

Network Security Manager

- Secure the ICT infrastructure against misuse or attack.
- Ensure filtering, monitoring, and password protection systems are effective.
- Monitor network and email use, reporting misuse to the DSL.
- Stay up to date with technical developments in e-safety.

Teaching and Support Staff

- Maintain up-to-date awareness of e-safety.
- Follow the Staff Acceptable Use Policy.
- Report concerns to the DSL or Network Manager.
- Embed e-safety into teaching and activities.
- Model responsible digital behaviour.
- Monitor ICT use in lessons and activities.
- Guide students to appropriate resources and manage unsuitable content.

Students

- Follow the Student Acceptable Use Policy.
- Report abuse, misuse, or inappropriate materials.
- Respect copyright and avoid plagiarism.
- Understand policies on mobile phones, cameras, images, and cyberbullying.
- Adopt safe online practices both inside and outside the Academy.

Parents and Carers

- Support their child's responsible use of technology.
- Endorse the Student Acceptable Use Policy.
- Access Academy systems in line with policy.
- Engage with Academy communications about e-safety (letters, newsletters, parents' evenings).

Education and Training

E-safety is an essential part of the Academy's safeguarding provision. Students, staff, and parents/carers will all be supported to develop the knowledge and skills needed to use technology responsibly and safely.

For Students

E-safety education will be delivered in the following ways:

- **Curriculum delivery** – through a planned e-safety programme within **PSHE** and other curriculum subjects, revisited regularly to reflect new technologies and emerging risks.
- **Key messages** – reinforced through assemblies, tutor sessions, and other whole-school activities.
- **Critical awareness** – teaching students to question and evaluate the content they access online and to validate information sources.
- **Acceptable Use** – ensuring all students understand and follow the Academy Acceptable Use Policy, adopting safe and responsible behaviours with ICT, the internet, and mobile devices both in and out of school.
- **Respect for copyright** – encouraging students to acknowledge information sources and respect copyright law.
- **Positive role models** – staff will model safe and responsible use of digital technologies at all times.

Parents and Carers

Parents and carers play a vital role in supporting their children's safe use of technology. Research highlights that:

- Many parents have only a limited understanding of online safety risks.
- Children and young people often encounter harmful or inappropriate material more frequently than adults realise.
- Parents may feel unsure how to respond to online safety concerns.

This "**generational digital divide**" (Byron Report) makes it essential that the Academy works in partnership with families. We will provide parents and carers with information, guidance, and opportunities to build their confidence in supporting their child's online safety.

The Academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents consultation and information evenings

All staff will receive e-safety training in order to understand their responsibilities, as outlined in the policy. Training may take the format of:

- A planned programme of formal e-safety training made available to staff via. The National College. It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy E-Safety Policy and Acceptable Use Policy
- Regular updates will be provided to all staff through ICT staff or the Designated Lead for Safeguarding and Child Protection, as required.

Curriculum

E-Safety should be a focus in all areas of the curriculum and should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Use of digital and video images – photographic, video

- Staff may take images for educational purposes only, using Academy equipment.
- Parental consent must be obtained before publishing images of students.
- Images must not cause embarrassment or bring the Academy into disrepute.
- Students must not take or share images of others without permission.
- Full names will not be published alongside images of students.

When using digital images, staff should inform and educate students about the rules and risks associated with the taking, use, sharing, publication and distribution of images.

- Staff are allowed to take digital / video images to support educational aims, but must follow Images of Children protocol concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes unless explicit permission has been given by the Principal – see Safeguarding Policy for further details
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals of the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with Images of Children protocol
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs unless complying with Images of Children protocol
- Written permission from parents or carers will be obtained before photographs of students are published on the Academy website

Data Protection

Personal data will be handled in line with the **UK GDPR and Data Protection Act 2018**. It must be:

- Fairly and lawfully processed
- Used only for specified purposes
- Adequate, relevant, and not excessive
- Accurate and up to date
- Kept no longer than necessary
- Processed securely
- Transferred only with adequate protection

Staff responsibilities include:

- Using secure, password-protected devices.
- Logging off when finished with personal data.
- Encrypting data when transferred.
- Ensuring portable devices are password-protected and malware-protected.
- Securely deleting data once it is no longer required.

Communications

When using communication technologies the Academy will consider the following as good practice:

- The official Academy email service may be regarded as safe and secure and is monitored
- Users need to be aware that email communications are monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) Academy systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications

- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff

Responding to incidents of misuse

- Misuse of ICT systems and digital technologies within the Academy may occur in different ways. It may be **careless**, through a lack of understanding or awareness of appropriate use; **irresponsible**, where behaviour shows poor judgement; or **deliberate**, where actions are intended to cause harm, disruption, or to access inappropriate or illegal content.
- Examples of serious misuse include, but are not limited to:
- Accessing, creating, or sharing **child sexual abuse images**
- Accessing or distributing **adult material** in breach of the *Obscene Publications Act*
- Viewing or promoting **racist, extremist, or radicalising material**
- Any other conduct that may be considered **illegal or criminal** in nature
- All incidents will be dealt with in accordance with **United Learning Safeguarding and Disciplinary procedures**, ensuring that responses are proportionate, consistent, and focused on safeguarding the welfare of students.

Sanctions

- The Academy operates a clear, staged approach to sanctions in response to e-safety breaches:
- **First breach** – normally results in a **written warning**, reinforcing expectations and reminding the student of their responsibilities under the Acceptable Use Policy. This stage is designed to be corrective and educational, helping students to understand why their behaviour was inappropriate.
- **Second breach (within the same term)** – will normally result in a **Senior Leadership Team (SLT) detention**, signalling the seriousness of repeated misuse and providing an opportunity for further reflection and reinforcement of e-safety principles.
- **Continued or repeated breaches** – may lead to the **removal of internet or ICT access privileges**, either temporarily or permanently depending on the severity of the incident. This step may impact a student's access to certain aspects of learning but is necessary where behaviour presents a continued risk.
- Where a student's online activity raises a **safeguarding concern** – for example, searching for harmful content, evidence of grooming, or attempts to bypass filtering to access dangerous material – the matter will be referred **immediately to the Designated Safeguarding Lead (DSL)**. In such cases, safeguarding considerations will always take precedence over disciplinary measures, and external agencies (including police or children's social care) may be contacted where appropriate.
- The Academy's approach to responding to misuse is based on the principle of **education first, sanction second**. Wherever possible, students will be supported to learn from mistakes and to build resilience in order to make safer choices online in the future. However, deliberate or repeated breaches will be treated with the necessary seriousness to protect the wider school community.

Checked by: Amy Houghton-Barnes, Assistant Principal, DSL	September 2025
Ratified:	October 2025
To be reviewed:	September 2026