



Online Safety (E-Safety) Policy

The Positive Impact Group

Effective Date

June 2026

Review Date

June 2027



Principles

This policy has been written for The Positive Impact Primary Academy, in line with local and national guidance. This policy should be read in conjunction with the Safeguarding and Child Protection Policy, the Anti-bullying Policy and the Curriculum Policy.

At The Positive Impact Group, we recognise both the significant benefits and potential risks associated with using the Internet and digital technologies. This policy outlines clear procedures to ensure that our pupils use these tools safely, responsibly, and with discernment. We believe that the ability to navigate the Internet safely is an essential life skill. Our aim is to empower pupils to understand existing risks, make informed choices, and confidently manage future challenges in a rapidly evolving digital world.

We also acknowledge that adults, both in their personal and professional lives, can be vulnerable to online threats, such as cyberbullying, phishing, or reputational harm. This policy emphasises the importance of training and promoting best practices among staff to ensure safer and more effective use of technology. In addition, we are aware of broader safety concerns related to technology use, including screen overexposure, privacy issues, and the impact of social media. These concerns are addressed through ongoing education, support, and practical guidance for both pupils and staff.

As new opportunities and risks emerge daily in the digital landscape, this policy will be reviewed regularly to remain current and effective. Our goal is to equip our pupils with the knowledge, skills, and confidence to use technology positively and safely.

E-Safety Coordinator for The Positive Impact Group

David Strong

Director of Operations

david.strong@positive-impactuk.com

Teaching and Learning

As we move towards a more digital curriculum, we will actively promote the use of 'real-world' technologies to enhance and support learning.

Why Internet Use is Important

- The Internet is an essential element in 21st-century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet Use Will Enhance Learning

- The Positive Impact Primary Academy's internet access has been designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught the differences between acceptable and unacceptable Internet use and given clear objectives for Internet use.
- The setting is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses strategies in learning resource areas where older pupils have more flexible access.
- In the event of pupils trying to make inappropriate use of the internet, particularly using search engines, this is captured and reported in real time. Senior staff will follow these up with pupils, notify their families and keep an incident record on the pupil's file for future reference as required.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation throughout the curriculum.

Pupils Will Be Taught How to Evaluate Internet Content

- The setting will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Good Practice

- Teaching staff will update and check websites before accessing them with the children to ensure that the content is appropriate. The curriculum is planned in context for internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required, e.g. Yahoo for kids or Ask for kids.
- Families provide consent for pupils to use the internet, as well as other ICT technologies.

- The setting makes clear that all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse, through staff meetings and the curriculum plans.
- A record is kept of any cyberbullying or inappropriate behaviour in line with the school behaviour management system. Parents/carers are informed of significant or repeated inappropriate behaviours.
- The setting ensures the Designated Safeguarding Lead Professional has appropriate training in E-Safety.
- The setting provides advice and information on reporting offensive materials, abuse/bullying etc and makes this available for pupils, staff and parents.
- E-Safety advice for pupils, staff and parents is provided annually.
- The setting ensures that when copying materials from the web, staff and pupils understand issues around plagiarism, how to check copyright and also know that they must observe and respect copyright / intellectual property rights.
- The setting ensures that staff and pupils understand the issues around aspects of the commercial use of the internet in an age-appropriate way. This may include risks in pop-ups, buying online, online gaming or gambling.
- The setting makes training on the E-Safety education available to staff.
- The setting provides advice, guidance and training for parents, including information leaflets; in school newsletters; on the website.

Managing Internet Access

Information System Security

- The Positive Impact Primary Academy's ICT systems capacity and security are reviewed regularly
- Virus protection is updated regularly

Email

- Pupils may only use approved school e-mail accounts on the school system.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school-headed paper.
- The forwarding of chain letters is not permitted.

Published Content and Website

- The contact details on the website are the school address, e-mail and telephone number. Staff, pupils' or governors' personal information will not be published.

- The Director's nominee will take overall editorial responsibility and ensure that content is accurate, appropriate, up to date and aligned to statutory requirements.

Publishing Pupils' Images and Work

- Photographs that include pupils will not refer to the pupil by name. Digital images/video of pupils stored in a teacher's documents or shared images folder on the network are deleted at the end of the year, unless specifically required for a key school publication or assessment information.
- Images of children and staff are not to be taken on or away from the setting premises by parents or visitors, unless prior permission is explicitly sought and given by the school or at scheduled school events.
- Pupils are not identified by their full name in online photographic materials or in the credits of any published video materials.
- Parental agreement is obtained through the specific confirmation of a consent form signed at the point of admission, before pupils' images are published on the website or other publications.

Social Networking and Personal Publishing

- The setting blocks and filters access to social networking sites or newsgroups unless there is a specific, approved educational purpose.
- Pupils are advised to be very careful about placing any personal photos on any social online network. They are taught to understand the need to maintain privacy settings so as not to make public personal information.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents are advised that the use of some social network spaces, for example, Facebook, Instagram, TikTok, Snapchat, WhatsApp, outside school is inappropriate for primary-aged pupils and that some of these sites have minimum age requirements.
- Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name of the file) that reveals the identity of others and their location, such as house number, street name or school. They are taught the need to keep their data secure and what to do if they are subject to bullying or abuse.

Managing Filtering

- The setting will work with relevant providers (in this case Warwickshire LA) to ensure systems which protect pupils are regularly reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Leader.
- The school will immediately refer any material we suspect is illegal to the appropriate authorities, e.g., the police and the local authority.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit, and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to GDPR requirements.

Policy Decisions

Authorising Internet Access

- The setting reserves the right to withdraw internet access from a pupil or member of staff in the event of misuse or infringement of policy.

Assessing Risks

- The setting will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can't accept liability for the material accessed or any consequences of Internet access.
- The setting will audit ICT provision annually to establish whether the E-Safety policy is adequate and whether its implementation is effective.

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Director.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

GDPR Compliance

The aim of GDPR legislation is to return control to individuals by allowing them to request deletion or disclosure of their data. As an educational setting, we have a responsibility to provide evidence of our data storage activities. In terms of E-Safety, the implications of this are as follows:

- The setting must annually ensure that its digitally held (and paper-based) storage of personal data is logged and that a list of the software used across the school (including teacher selected APPs) is GDPR compliant.
- Staff need to check what data is being extracted by all online tools / APPs used and that this is in line with GDPR requirements.
- The setting must have a lawful basis for processing personal data.
- Parents must complete a data use consent form each year.
- The setting must have a privacy policy on the website, which must be distributed to all staff.
- There should be clear procedures in place to find, delete and disclose relevant data as required. Warwickshire IT services provide a helpdesk service for schools regarding the legal and timely deletion of data.
- The setting must appoint a Data Protection Officer (David Strong).

Communications Policy

Introducing the E-Safety Policy to Pupils

- E-safety rules are displayed in work areas and are discussed with the pupils on a regular basis.
- Pupils are informed that network and internet use will be monitored.
- Pupils are not allowed to use mobile phones in The Positive Impact Primary Academy. Upon entering the site, children's mobile phones must be turned off and handed into the pupil's Education Mentor. They will be stored safely in the staff office and returned to the children at the end of the day.

- The use of a smartwatch is also not permitted.

Staff and the E-Safety Policy

- The E-Safety Policy is distributed to all staff and is included in child protection training sessions.
- Internet usage is able to be monitored and can be traced to the individual user.
- Discretion and professional conduct are essential.

Enlisting Parents' Support

- Parents/carers' attention will be drawn to the setting's E-Safety Policy in a variety of ways, including newsletters, open evening events and on the website.

This policy is reviewed annually.

Overall responsibility lies with the Director, who liaises with the Senior Leadership Team to ensure a robust and sustainable model of Leadership.

Signed by Director



James Armson

