# ASTON FENCE J & I SCHOOL

## E-SAFETY POLICY

**February 2023**

# E-Safety Policy

**Date: February 2023**
**Review Date: February 2024**

## Introduction

At Aston Fence J & I School, we feel that the Internet and other technologies have an important role to play in the learning and teaching process and support achievements in all areas of a child's life while in education and beyond into adulthood. Aston Fence J & I School is committed to providing all children with opportunities to develop their computing knowledge, skills and understanding confidently, competently and safely in their learning and in everyday contexts. Children are encouraged to become independent and astute users of technology, recognising both opportunities and risks and using strategies to stay safe. This eSafety policy reflects the school's commitment to their safeguarding and well-being.

## Responsibilities of the School Community

We believe that eSafety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

### Responsibilities of the Management Team

- Develop and promote an eSafety culture within the school community.
- Support the eSafety coordinator in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafety effectively.
- Receive and regularly review eSafety incident logs and be aware of the procedure to be followed should an eSafety incident occur in school.
- Take ultimate responsibility for the eSafety of the school community.

### Responsibilities of the eSafety Coordinator

- Promote an awareness and commitment to eSafety throughout the school.
- Be the first point of contact in school on all eSafety matters.
- Create and maintain eSafety policies and procedures.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in eSafety issues.
- Ensure that eSafety education is embedded across the curriculum.
- Ensure that eSafety is promoted to parents and carers at least annually and in response to current events or issues.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on eSafety issues to the SMT and governors as appropriate.
- Ensure an eSafety incident log is kept up-to-date.
- Keep up to date with new technologies and their potential for inappropriate use by pupils and staff.

**Responsibilities of Teachers and Support Staff**

- Read, understand and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff AUP (Acceptable User Policy).
- Develop and maintain an awareness of current eSafety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed eSafety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- **All pupils** working in the Computing Suite or on remote devices must be supervised by an adult at all times including indirect supervision.
- Be aware of what to do if an eSafety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Be aware of and alert to the potential signs of online grooming and child sexual exploitation.
- Introduce the AUP and eSafeguarding policy at the start of every school year.

**Responsibilties of Technical Staff**

- Read, understand, contribute to and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff AUP.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school computing system.
- Report any eSafety-related issues that come to your attention to the eSafety coordinator.
- Develop and maintain an awareness of current eSafety issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.

**Responsibilities of Pupils**

- Read, understand and adhere to the school pupil AUP.
- Help and support the school in creating eSafety policies and practices and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss eSafety issues with family and friends in an open and honest way.

**Responsibilities of Parents and Carers**

- Help and support your school in promoting eSafety.
- Read, understand and promote the school pupil AUP with your children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.

- Are responsible for resolving any issues arising from their child using technologies, including social media, outside of school.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss eSafety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of technology.

**Responsibilities of Governing Body**

- The school has appointed a member of the Governing Body to take lead responsibility for eSafeguarding.
- Read, understand, contribute to and help promote the school's eSafety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
- Develop an overview of how the school computing infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety activities.
- Ensure appropriate funding and resources are available for the school to implement their eSafety strategy.

**Learning and Teaching**

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

- We will provide a series of specific eSafety-related lessons in every year group as part of the computing curriculum, PSHE curriculum and other lessons.
- We will celebrate and promote eSafety through whole-school and individual class activities.
- We will discuss, remind or raise relevant eSafety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- We will remind pupils about their responsibilities through an end-user AUP which will be displayed throughout the school.

- Staff will model safe and responsible behaviour in their own use of technology during lessons.

**How parents and carers will be involved**

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Include useful links and advice on eSafety regularly in newsletters and on our school website/Twitter feed.
- Include a section on eSafety in the School Prospectus.
- Ask parents to read the Acceptable User Policy, discuss it with their children and sign it.
- School will provide up-to-date training/advice on how to keep children safe online at home eg. eSafety Coffee Morning, Webinar.
- Promote free registration to National Online Safety, where training and up to date guidance and information can be accessed.

**Managing Computing Systems and Access**

Internet access is provided by Impelling, who ensures that access is a safe as possible. The school infrastructure, hardware and software are also managed by Impelling.

- The school will be responsible for ensuring that access to the computing systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school computing systems, and that such activity will be monitored and checked.
- At KS1 pupils will access the computers using an individual log-on, which the teacher supervises. All Internet access will be by working alongside a member of staff, or if working independently a member of staff will supervise at all times.
- At KS2 pupils will access the computers using an individual log-on, which they will keep secure. Internet access will be supervised by a member of staff.
- Members of staff will use only school USB drives to transfer data between school and teacher laptops. These will be encrypted with a password to prevent loss of confidential data.
- Any administrator or master passwords for school computing systems should be kept secure and available to at least two members of staff, e.g. head teacher and member of technical support.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.

- The school will regularly audit computing use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.
- Users using the unfiltered 'Guest' internet will agree to terms of use.

**Filtering Internet access**

- The school uses a filtered Internet service. The filtering is provided through Study Safe and is password protected.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafety coordinator.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafety coordinator. The school will report this to appropriate agencies including the filtering provider, LA and CEOP .
- The school infrastructure, hardware and software is managed by Impelling.

## Learning technologies in school

| | **Pupils** | **Staff** |
|---|---|---|
| **Personal mobile phones brought into school** | Allowed with permission Switched off at all times | Allowed |
| **Mobile phones used in lessons inc. smart watches** | Not allowed | Not allowed |
| **Mobile phones used outside of lessons** | Not allowed | Allowed |
| **Taking photographs or videos on personal equipment** | Allowed on residential visits with no subsequent internet postings | Allowed for selected staff |
| **Taking photographs or videos on school devices** | Allowed | Allowed |
| **Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles** | Not allowed | Allowed at certain times |
| **Use of personal email addresses in school** | Not allowed | Allowed |
| **Use of school email address for personal correspondence** | Not allowed | Discouraged |
| **Use of online chat rooms** | Not allowed | Not allowed |
| **Use of instant messaging services** | Not allowed | Not allowed |
| **Use of blogs, augmented reality, podcasts** | Allowed | Allowed |
| **Use of video conferencing or other online video meetings** | Allowed with supervision | Allowed |
| **Use of social networking sites** | Not allowed | Not allowed |

**Using Email and Social Networking in and outside school**

- Staff should use approved e-mail accounts allocated to them by the school and be aware that their use of the school e-mail system will be monitored and checked.
- Pupils are not permitted to access personal e-mail accounts in school.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.
- No comments are to be made regarding any aspect of work, including pupils and colleagues.
- Staff using social networking sites are not to have any contact with anyone under the age of 18 who they know through a work capacity.

**Using images, video and sound**

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will only be created using equipment provided by the school.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff or pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

**Using mobile phones**

- Personal mobile phones will not be used during lessons by pupils or staff. This includes the use of smart watches.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, they should do so via school and/or with personal number withheld.
- Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

**Using new technologies**

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafety point of view.
- We will regularly amend the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafety risk.

**Protecting personal data**

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.

- Staff will not remove personal or sensitive data from the school premises without permission of the head teacher, and without ensuring such data is kept secure.

**The school website and other online content published by the school**

- The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
- A generic contact e-mail address and online form will be used for all enquiries received through the school website.
- The school website will not include photographs of any children where parents have specifically asked for their exclusion.
- The school website will not include photographs of staff without prior permission.