Pathways School

E-Safety Policy

Policy Monitoring

Date of last review: September 2022

Reviewed by: Saima Ali Majid, Chair of Trustees

Neil Jones, Headteacher

Date of next review: September 2023

This policy will be reviewed at least annually and following any concerns and/or updates to national/local guidance or procedure.

1. Introduction

E-safety can be very broadly defined as the safe use of technology. Technology is a broad term. More specifically, e-safety can also be called ‘internet safety,’ ‘online safety’ or ‘web safety.’ This includes the use of the internet and other means of communication or accessing data or information using electronic media (e.g., text messages, gaming devices, email etc). In practice, e-safety is as much about behaviour as it is electronic security.

2. Areas of Risk

E-safety in this context can be classified into three areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful material;
- Contact: being subjected to harmful online interaction with other users;
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

This E-safety Policy recognises the commitment of Pathways School to E-safety for all. We can all benefit from the opportunities provided by the Internet and other technologies used in everyday life. The E-safety Policy supports this by identifying the risks and the mitigating actions we are taking to avoid them.

3. Links to other school policies and practices

- Data Protection Policy;
- Privacy Policy;
- Staff Code of Conduct;
- Disciplinary, Conduct and Grievance Policy;
- Child Safeguarding Policy and Procedure;
- Safeguarding Adults at Risk Policy and Procedure.

4. Legislation

- Data Protection Act 2018 and the associated General Data Protection Regulations (GDPR);
- Computer Misuse and Cybercrimes Act;
- Regulations of Investigatory Powers Act;
- Obscene Publications Act;
- Copyright, Design and Patents Act;
- Communications Act;
- Digital Economy Act.

5. Roles and Responsibilities

5.1 The Headteacher

The Headteacher has a duty of care for ensuring the safety (including E-safety) of members of the school community. This responsibility is additionally delegated to all

teaching and support staff involved with any teaching and learning involving the use of IT. The Headteacher needs to:

- be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- ensure that relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- ensure that there is a system in place to allow for monitoring and support of those in the school who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

5.2 Designated Safeguarding Lead (Currently the Headteacher)

The Designated Safeguarding Lead (DSL) is trained in e-safety issues and is aware of the potential for serious safeguarding issues to arise from:

- sharing of personal or confidential data.
- access to, viewing of or sharing illegal/inappropriate material.
- inappropriate online contact with adults/strangers.
- potential or actual incidents of grooming.
- cyber-bullying.
- scams.

The DSL will:

- Create and maintain the school's E-safety Policy.
- Refer all e-safety incidents to the relevant safeguarding lead and assist them as required.
- Receive reports of E-safety incidents and assist, signpost or refer as appropriate.
- Ensure the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensure that users may only access networks, resources, and devices through an enforced password protection system.
- Ensure the use of multi-factor authentication when accessing the school's systems or devices remotely.
- Keep up to date with E-safety technical information to effectively carry out their E-safety role and to inform and update others as relevant.
- Monitor the use of the network, internet, email, and software solutions in order that any misuse or attempted misuse can be reported to the relevant safeguarding lead.
- Ensure that monitoring software/systems are appropriately implemented and updated regularly.

5.3 All Staff

The staff will:

- Ensure they have read the school's E-safety Policy.

- Ensure have read, understood, and signed the ICT Acceptable Usage Policy (Staff and Volunteers).
- Ensure report any suspected misuse or problem to the Headteacher.
- Ensure students understand and follow the e-safety and Acceptable Usage Agreements.
- Monitor the use of devices and digital technology at work, in lessons and other activities using appropriate security system and software solutions and implement current policies about these devices.

In lessons where internet use is pre-planned, students should be guided to websites or other networked on online resources checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

5.4 Parents and Carers

Parents and Carers play a crucial role in ensuring that their children or young adults in their care understand the need to use the internet and computer or mobile devices in an appropriate way. The schools and college will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school and college events;
- children and young peoples' personal or mobile devices in the school and college (where this is allowed).

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

- Curriculum activities;
- Letters, newsletters, school websites;
- Parents/Carers evenings/sessions;
- High profile events/campaigns e.g., Safer Internet Day.

6. Policy Statement

6.1 Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in E-safety is therefore an essential part of the E-safety provision. Students at Pathways need significant help and support to recognise and avoid e-safety and online risks and build their online resilience. Some students due to levels of understanding will not be able to build their own protections and this will form part of the student's individual risk assessment.

E-Safety is a focus in all areas of the curriculum as appropriate, and staff reinforce E-safety messages throughout. The E-safety curriculum is provided in the following ways:

- Planned E-safety content in teaching.
- Key E-safety messages are repeatedly reinforced as part of a planned programme of training activities.
- Students are taught to be aware of the content they access online and are guided where possible to question and validate the accuracy of information.
- Students are taught where possible to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students are helped to understand and are encouraged to adopt safe and responsible use of the internet and social media both within and outside the school.
- Staff act as good role-models in their use of digital technologies, the internet, and mobile devices.
- In lessons where internet use is pre-planned, students are guided to websites or online resources which have been pre-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, staff should be vigilant in monitoring the content of the websites the young people visit.
- Any request to block or unblock an internet site, should be recorded, with clear reasons for the need and shared with the Headteacher.

6.3 Staff and Volunteers

As part of their induction, all new staff and volunteers must familiarise themselves with the school's E-safety policy and review and complete the ICT Acceptable Usage Agreement.

This E-safety policy and its updates should be presented and discussed by staff in staff team meetings/INSET days, school meetings.

A planned programme of formal E-safety training should be made available to staff as required.

7. Mobile Phones and Portable Devices Provided by the school

The school issues mobile phones and tablets to some of its employees based on job requirements. Where such a device has been issued, it is primarily for business use and always will remain the property of the school. The user will be responsible for its safekeeping, appropriate use, condition, and eventual return to the school. If a device is lost or stolen this should be reported to the Headteacher.

Bring Your Own Device (BYOD) – Staff and Volunteers Staff and volunteers may bring their own personal, electronic devices into work settings. These may include mobile phones, laptops, or tablets. The school provides internet access through its wireless networks at no cost to staff. When accessing the network or using a personal mobile electronic device within the school's settings, staff and volunteers

must abide by this E-Safety Policy, as well as the IT Acceptable Usage Policy. Work-related activity should be completed on a school device when possible. Staff and volunteers bring their devices to the school at their own risk. The use of a personal mobile or electronic device by staff is strictly not allowed in classrooms or teaching environments, or at any point when working with students accept with written permission from the Headteacher.

8. Data Protection

An essential E-safety consideration is that everyone covered by this policy should have a working awareness of the UK-GDPR. GDPR stands for General Data Protection Regulations. This is to prevent a data breach or any processing of personal data that is not compliant with the law. Students where possible should be supported to understand their rights under the UK-GDPR as part of the school's E-safety provision. The staff is made of aware of their responsibilities regarding the UK-GDPR. They understand the lawful basis under which they can access, process, or share data (which will be included in process documentation) - whether it be contractual, legitimate interest or consent - and understand what a data breach is and recognise a subject access request.

9. Using Digital and Video Images

Making and using digital and video images can provide benefits in the school. However, staff, parents, carers, and students need to be aware of the risks associated with publishing digital images on the internet, or social media platforms. Such images may provide avenues for cyberbullying to take place or attract other undesirable or inappropriate attention. Such images may in some instances provide detail or information which could be used to identify a young person’s whereabouts, and all staff and parents should be aware of this risk. Digital images may remain available on the internet indefinitely and may cause harm or embarrassment to individuals in the short or longer term. When using or working with (making) digital images or video, staff should inform and educate students about the risks associated with the taking, use of, sharing, publication and distribution of digital content or material. They should recognise the risks attached to publishing their own images on the internet e.g., on social media platforms. Parents and carers are welcome to take videos and digital images of their child or young adult at school events for their own personal use but should not video other children. To respect the privacy of pupils and learners, these images should not be published or made publicly available on social media platforms nor should parents and carers comment on any activities involving other learners or pupils in the digital or video images. Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow the school’s policy concerning the sharing, distribution, and publication of those images. Images should only be taken on the school’s equipment. Care should be taken when taking digital or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute or lead to any breach of our Code of Conduct or Safeguarding Policies.

Written permission from parents and carers, or where appropriate, students, will be obtained before photographs, video or other media are published.

10. Prevent Duty

The school is committed to providing a safe and secure environment for its students. Staff and volunteers are trained in safeguarding processes relating to Prevent Duty, and the risk of extremism or radicalisation due to the use of the internet or social media.

11. Additional Support

Additional support can be sought at the UK Safer Internet Centre's helpline for professionals:

Email helpline@saferinternet.org.uk

Telephone: 0344 381 4772