Internet Safety Policy

July 2024

1. Policy statement
Our Internet Safety Policy should be read in conjunction with other related school policies and documents. In particular, this document will be used in conjunction with the Frays Academy Trust Behaviour Policy, Safeguarding Policy, IT Acceptable Use Agreement and Anti-Bullying Policy.

2. Policy aims
The schools within the Frays Academy Trust provide a rich and broad approach to the use of technology to support pupils' learning. We aim to ensure that children's learning is enhanced by the use of such technology, and that children are equipped with the skills and knowledge to use technology appropriately and responsibly. We believe that children must be taught to recognise the risks associated with technology and how to deal with them, both within and outside the school environment. Above all, we aim to ensure that all children are protected from harm when using the internet. We ensure that all members of the school community understand their role in keeping children safe online.

3. The role of the Senior Leadership Team
The role of the Senior Leadership Team and ICT Leader include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Internet Safety Policy and associated policies
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring that any internet safety incidents are effectively investigated and resolved
- Keeping personally up-to-date with Internet Safety issues and guidance
- Providing or arranging Internet Safety advice/training for staff, parents/carers and governors
- Liaising closely with the school's Designated Safeguarding Lead to ensure a co-ordinated approach between internet safety and safeguarding

4. Policies and Practices
This section of the Internet Safety Policy sets out the school's approach to internet safety along with the various procedures to be followed in the event of an incident.

4.1 Security and data management
All data in the school is kept secure, in accordance with the Internet Safety Policy and IT Acceptable Use Agreement. Staff are made aware of this as part of induction, and through regular training. The IT Acceptable Use Agreement should be signed by staff annually.

4.2 Use of mobile devices
The use of mobile devices such as iPads, Chromebooks, laptops or Kindles, offers a range of opportunities to extend children's learning. Staff are aware that some mobile devices e.g. mobile phones, game consoles or smart watches can access unfiltered internet content and therefore may pose a risk to children.

- Mobile devices are not encouraged to be brought into school by children.
- Any phones brought to school by children who walk home alone and require them for safety reasons should be turned off, locked away during the school day and not used by children whilst on school property.
- Children must have a permission slip to bring in a mobile phone.
- Children are not permitted to bring games consoles or personal tablets into school.
- Children are not permitted to wear smart watches that are able to connect to the internet.

4.3 Use of digital media
Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using,

sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure, school Facebook or display.

- At school photographs and videos of pupils and staff are regarded as personal data, and the school has written permission for their use from their parents or carers
- The school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used
- The parental/carer written permission is obtained by the school office but the parents have a right to change this at any time
- The staff and pupils aware that full names and personal details will not be used on any digital media, particularly in association with photographs
- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs. Parents /carers are however reminded not to publish these images on social media if they contain images of children who are not their own.
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- The school ensures that photographs/videos are only taken for school purposes only
- Permission is sought from the Headteacher before staff use their own cameras/smartphones for the purposes of taking photos or videos and are immediately transferred to a school based system, deleted and not stored on their device.
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils
- Staff are encouraged not to store digital content on personal equipment.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.

4.4 Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks.

Email

- All staff have access to the London Grid for Learning service as the preferred school e- mail system.
    - This email system should be used by staff in accordance with the IT Acceptable Use Agreement.

Social Networks

Social Network sites should be used by staff in accordance with the IT Acceptable Use Agreement.

Apps

Smart phones are increasingly being used by younger children today. These allow children a range of access to people around the world, allowing them to publish pictures, communicate and share information. Staff need to raise awareness of the risks involved to children and educate them on the correct usage and guidance.

- Children should be aware of the ages required to use different platforms such as;
    - Snapchat
    - Tik Tok
    - Youtube
    - Facebook
    - WhatsApp
- Adults must not communicate with pupils using any apps.
- Pupils should be aware of the potential dangers of using apps and have guidance on how to report any misuse or concerning content.

E-Learning Platforms

Schools use site including (but not limited to), Purple mash and TT Rockstars as their online learning

platforms.

- Children will be given access to TT Rockstars and Purple Mash accounts, but SLT will have access and admin rights across the learning platform.
- Passwords are issued to the children and they are taught not to share their password, and the reasons for this.
- Pupils are taught to use these communication tools in a responsible way in conjunction with the e-safety curriculum.
- Teachers know how to use and monitor TT Rockstars and Purple Mash. Teaching staff will have administration rights within their own class.
- Any safeguarding concerns would be reported to the DSL in accordance to safeguarding procedures.
- Accounts are kept historically on the server however are made inactive by the administrator. This is completed annually.

Others
The School will adapt/update the Internet Safety policy in light of emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared communication.

4.5 IT Acceptable Use Agreement
Our IT Acceptable Use Agreement is intended to ensure that users of technology within school will be responsible and stay safe. It ensures that users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

Our IT Acceptable Use Agreement is used for staff must be signed and adhered to by users before access to technology is allowed.

4.6 Dealing with incidents
Any e-safety concerns will be reported and dealt with in accordance with the Child Protection Policy and Behaviour Policy.

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Staff will not personally investigate, interfere with or share evidence to avoid inadvertently committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to appropriate agencies.
Examples of illegal offences are:
- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

Any allegations of staff inappropriate or illegal use of technology will be dealt with by the Headteacher in accordance with the Child Protection Policy and the Dealing with Allegations of Abuse towards Teachers and Staff policy, and the LADO will be informed.

Inappropriate use
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The SLT will decide what constitutes inappropriate use and the sanctions to be applied in line with the Behaviour Policy.

5. Infrastructure and Technology
The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection are in place.

Pupil access
- The children are supervised by staff when accessing school equipment and online materials

Passwords
- All users of the school network have a secure username and password.
- The administrator password for the school network available to the Headteacher and other nominated senior leader is kept in a secure place (this must be authorised by the Executive Headteacher).
- Staff and pupils are reminded of the importance of keeping passwords secure.
- Passwords will only be changed if the need arises.

Software/hardware
The school has legal ownership of all software.
The school has an up to date record of appropriate licences for all software

Managing the network and technical support
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Waterman Solutions/School is responsible for managing the security of the school network.
- The safety and security of the school network is monitored on a regular basis.
- The school systems are kept up to date in terms of security e.g computers are regularly updated with critical software updates/patches.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password.
- Staff and pupils are encouraged to lock or log out of a school system when a computer/digital device is left unattended.
- Only the administrator is allowed to download executable files and install software.
- Users report any suspicion or evidence of a breach of security to the SLT
- The school encourages staff not to use removable storage devices on school equipment e.g. encrypted pen drives.
- The school encourages teachers to follow IT Acceptable Use Agreement guidelines when using their school laptop at home
- If network monitoring takes place, it is in accordance with GDPR
- All internal/external technical support providers are aware of your schools requirements / standards regarding e-safety
- The office staff are responsible for liaising with Waterman Solutions for technical support.

6. Teaching and Learning
6.1 e-Safety Curriculum
- E-safety is embedded within the computing curriculum, as well as being taught explicitly in Computing and Wellbeing and Citizenship lessons.
- E-safety lessons can be taught at any time, depending on the needs and requirements of a class or cohort of children.
- All children, including those with educational needs, have access to the E-Safety curriculum.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.

6.2 Use of ICT across the curriculum

- ICT is used to enhance learning across the curriculum
- Children are signposted to appropriate search engines and website by teachers
- Any websites or links used are vetted by staff prior to the lesson taking place
- Children's use of ICT, particularly the Internet, is monitored by staff throughout the lesson

6.3 Use of ICT for home learning

- Home learning may be set online in the event of a school closure
- Staff will use TT Rockstars and Purple Mash to set tasks for home learning
- Any websites, resources or platforms signposted will be vetted by staff prior to the content being uploaded
- Any websites, resources or platforms signposted will be age appropriate and in line with the school's vision and ethos
- Any websites, resources or platforms signposted will be GDPR compliant
- Any and all pupil activity on TT Rockstars and Purple Mash will be regularly monitored by staff.
- Staff will not enter into private messaging with children on any platform, including social media
- Parents will receive appropriate support in enabling their child to access home learning

Pupils are reminded of safe Internet use e.g. classroom displays, e-safety rules and E-Safety Day. Schools will also signpost children to age appropriate practical support, such as Childline.

7 Internet Safety awareness in our community

7.1 Staff awareness

- There is a programme of formal e-safety training for all staff to ensure they are regularly updated on their responsibilities
- The SLT and ICT Leader provides advice/guidance or training to individuals as and when required.
- The Internet Safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Internet Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Internet Safety Policy and IT Acceptable Use Agreement
- Regular updates on Internet Safety Policy, IT Acceptable Use Agreement, curriculum resources and general e-safety issues are discussed in staff/team meetings.
- Staff are aware that the internet can be used as a tool to abuse children, and can be a platform for abuse including Child Sexual Exploitation, Child Criminal Exploitation, Sexual Abuse and Radicalization. Staff are trained in how to identify when children may be at risk in line with the Child Protection Policy.

7.2 Parent/carers' awareness

The school offers opportunities for parents/carers and the wider community to be informed about e-safety, including the benefits and risks of using various technologies. For example through:

- School newsletters, school website and other publications.
- Promotion of external e-safety resources/online materials.

7.3 Governors' awareness

The school considers how Governors, particularly those with specific responsibilities for Safeguarding, are kept up to date. This is through discussion at Governor meetings and Governor training.