William Henry Smith Foundation

E-Safety Policy

Policy Details

Status:	**In-house**
Frequency of review:	**Annually**
Lead member of staff:	**Damien Talbot**
Responsibility of:	**Thomas Forsyth**
Last reviewed:	**Spring 2025**
Next Review Date:	**Spring 2026**
Policy Number:	**FWS9**

1.0 Rationale

It is the duty of the foundation to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, children are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

using technology. This policy, supported by the Acceptable Use Policies (AUP) for staff and children and young adults, is to protect the interests and safety of the whole foundation community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. Both this policy and the Acceptable Use Policies (for all staff and Children and Young Adults are inclusive of both fixed and mobile internet, technologies provided by the foundation (such as PCs, laptops, whiteboards, tablet, digital video and camera equipment, etc.) and technologies owned by children and young adults or staff that connect to our WIFI. In line with the National Minimum Standards for Residential Special Schools 2022, this policy aims to ensure that children and young adults are safeguarded from potentially harmful and inappropriate online material also having regard to the Department's Keeping Children Safe in Education guidance in respect of the approach to harmful online content and how children and young adults devices are managed in the foundation.

2.0 The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used within the foundation and, more importantly in many cases, used outside of the foundation by children include:

- The Internet
- E-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

3.0 Whole foundation approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this foundation:

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

1. An effective range of technological tools which are filtered and monitored
2. Policies and procedures, with clear roles and responsibilities
3. A comprehensive E-Safety education programme for children and young adults, staff and parents.

4.0 Staff Responsibilities

E-Safety is recognised as an essential aspect of the foundation community and the CP / ICT team along with governors to bring these practices into the culture of the foundation. The SLT ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any E-Safety issues which may arise in classrooms or care on a daily basis. The ICT/CP Team are responsible for overseeing E-Safety across the foundation and dealing with any concerns via the appropriate means.

5.0 Staff Awareness

- All staff receive information and training on E-Safety issues in the form of in-house induction and meeting time alongside CEOP training run in house.
- New staff receive information on the foundation's AUP (Acceptable Use Policy) as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the foundation community.
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum and care areas and through a culture of talking about issues as they arise.
- E-Safety records of concern are completed by staff as soon as incidents occur and are reported directly to the foundation's designated safeguarding team and logged on SID / CP Folder on the shared drive which is restricted to CP team only
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms, care settings and other settings across the foundation and following the foundation E-Safety procedures. These behaviours are summarised in the AUPs which must be signed by staff and for children and young adults children and young adults, age appropriate online safety signage is displayed across site.

6.0 Internet

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

- We use a filtered Internet Service, which minimises the chances of children and young adults encountering undesirable material. Furthermore; any information that is deemed inappropriate is sent in an auto alert to the team by email including terrorism, pornography, prevent and radicalisation categories – this runs alongside regular manual checks by the ICT team both random and to any children and young adults placed on CP watch.
- Staff and children and young adults have access to the internet through the foundation's fixed and mobile internet technology.
- Staff should email foundation-related information using their designated foundation address and not personal accounts. If information is to be sent via email to an external person, service or provider, staff must ensure it is sent encrypted.
- Staff will preview any potential high-risk websites before recommending to children and young adults.
- If internet research is set for homework, specific sites that have been suggested should be checked by the teacher.
- Children and young adults accessing the internet via foundation devices and computers are presented with an acceptable use policy prior logging on.
- Children and young adults bringing in devices are allowed to access the internet outside of school hours by using our filtered wi-fi.
- E-Safety information is found on the foundation website as well as links to CEOPs website.
- If staff or children and young adults discover an unsuitable site, the screen must be switched off immediately and the incident reported to the ICT Team. The filter can then be investigated and improved further.
- Staff and children and young adults are aware that foundation-based email and internet activity is monitored and can be explored further if required.
- Children and young adults using the World Wide Web are expected not to deliberately seek out offensive materials. Should any children and young adults encounter any such material accidentally, they are expected to report it immediately to a teacher and then the Head of IT so that the Service Provider can block further access to the site.
- Children and young adults are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved. They are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Children and young adults consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the foundation's behaviour policy.

7.0 Passwords

- Use a strong password (strong passwords are usually eight characters or more and contain upper- and lower-case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.
- Two factor authentication is used for access offsite.

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

8.0 Data storage

- Staff are expected to save all data relating to their work to, SID or on the foundation server. This is to facilitate back up and easy recovery of information.
- We use Office Message Encryption to share email for any sensitive information e.g. pupil statements, contracts etc. to be sent to external people.
- Assessment records, contracts, staff/pupil medical information and any other data related to children and young adults or staff must not be stored on personal memory devices. The foundation systems including remote desktop services should be used for this.
- School allow the use of removable media if related to lesson or appropriate job content and not personal/sensitive information. However, staff who require regular access to information can do this via secure external links to SID or remote desktop.

9.0 Social Networking sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer or others to see.
- Staff roles in the foundation requires a high degree of professionalism and confidentiality. Staff do not give out personal contact information to children and parents of children whilst at WHSS. If necessary, only give out the foundation contact details.
- Any communications or content you publish that causes damage to the Foundation, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the Foundation Dismissal and Disciplinary Policies apply.
- The foundation expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use. Any communications made in a professional capacity through social media must not either knowingly or recklessly:
    - place a child or young person at risk of harm;
    - bring the Foundation into disrepute;
    - breach confidentiality;
    - breach copyright;
    - breach General Data Protection Regulations legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age; or using social media to bully another individual; or posting images that are discriminatory or offensive or links to such content.

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

10.0 Digital images

- Use only digital cameras, iPad, phones and video cameras provided by the foundation and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children.
- Ensure you are aware of the children whose parents/guardians have not given permission for their child's image to be used in or out of school. An up to date list is kept in the school administrative office and given to all staff.
- When using children's images for any school activity, they should not be identified by their full name. We do try and not use any name that will help with identifying any individual.

11.0 Proving a comprehensive E-Safety education to all children and young adults and parents

- All staff working with children must share a collective responsibility to provide E-Safety education to children and young adults and to promote E-Safety in their own actions.
- Formally, an E-Safety education is provided by the objectives contained in the ICT unit plans for every area of work for each year group. Even if E-Safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the Computing curriculum.
- Informally, a talking culture is encouraged in classrooms that allows E-Safety issues to be addressed as and when they arise. Also, staff are accessible at all times and will work with children and families to address any E-Safety issues.
- Staff will ensure children know to report abuse using the CEOP button widely available on many websites or to speak to any member of staff, who will escalate the concern to the person with responsibility for E-Safety.
- In line with our preventing extremism and radicalisation policy, we will ensure that children are safe from terrorist and extremist material when accessing the internet in school.

12.0 CCTV and Monitoring

12.1 The school has CCTV on the premises as part of site surveillance for staff and children and young adults safety. Recordings (which are retained by the support provider for 28 days) will not be revealed without permission of Senior Leadership except where disclosed to the police as part of a criminal investigation.

12.2 The Senior on Call may view CCTV as part of their duty when a child goes missing. This is only to be used to identify which direction a child may have left site, to support the child's safe return. SLT will be informed of all occasions when CCTV has been accessed.

12.3 Specialist lesson recording equipment may be used on occasion as a tool to share best teaching practice. These recordings are only accessible to authorised members of staff, following approval from the Senior Leadership Team and will not be used for any other purposes.

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

13.0 Maintaining the security of the foundation ICT Network

The foundations' ICT Support team maintains the security of the foundation network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the ICT users to uphold the security and integrity of the network by not accessing inappropriate sites and bringing in unsuitable materials such as viruses.

14.0 Monitoring

- The SLT/ Head of IT or other authorised members of staff may inspect or monitor any ICT equipment owned by the foundation at any time without prior notice.
- In line with KCSIE we have Smoothwall Filtering and monitoring in place for our filtering to flag up any keywords relating to radicalisation, abuse and other categories as listed in the appendix of this policy. See flowchart in appendix for our process in dealing with any content issues.
- Monitoring includes: intercept, access, inspect, record and disclose emails, instant messaging, internet/intranet use and any other electronic communications (data, email, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain Foundation business related information; to confirm or investigate compliance with Foundation policies, standards and procedures, to ensure the effective operation of Foundation ICT, for quality control or training purposes, to comply with a Subject Access Request under the General Data Protection Regulations, or to prevent or detect crime.

15.0 Breaches of Policy

Any policy breaches are grounds for disciplinary action. Policy breaches may also lead to criminal or civil proceedings. All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Designated Safeguarding Officers or Principal.

<u>Appendix</u>

Key word Categories Flagged up:

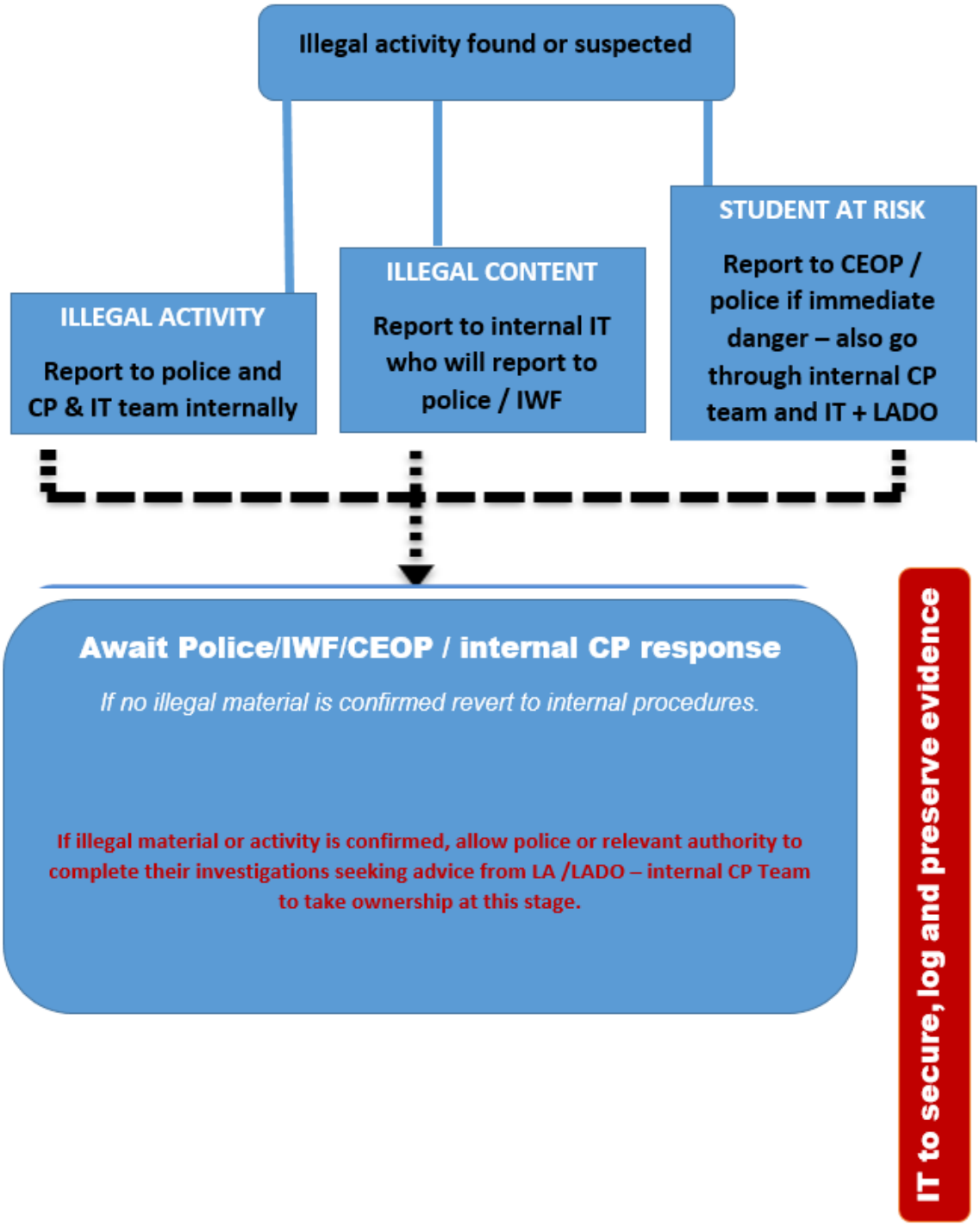
** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

Name	Type	Interval
Abuse References		Daily
Anxiety		Daily
Bullying References		Daily
Discrimination References		Daily
Drug References		Daily
Eating Disorder References		Daily
Hacking references		Daily
Mental Health References		Daily
Piracy and Copyright References		Daily
Pornography		Daily
Radicalisation		Daily
Sexual References		Daily
Terror Keywords		Hourly
Violence References		Daily
White Supremacy		Daily

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

Flowchart of dealing with e-safety issues

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*



** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*

** where there is a reference to children and young adults, we are including children in the Home/students in School and learners in College.*