FINBOROUGH MOBILE AND SMART TECHNOLOGY POLICY 2023

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

This policy has been written by Finborough School, taking into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, Early Years and Foundation Stage 2021, 'Working Together to Safeguard Children' 2018) and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

The purpose of this policy is to safeguard and promote the welfare of all members of the Finborough School community when using mobile devices and smart technology and highlight the critical importance of sustained good digital character as set out in our iTrust approach.

Finborough recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all children and staff are protected from potential harm when using mobile and smart technology.

As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), is recognised as having overall responsibility for online safety.

This policy applies to all access to and use of all mobile and smart technology on site; this includes mobile phones and personal devices such as tablets, e- readers, games consoles and wearable technology, such as 'smart watches and fitness trackers, which facilitate communication or have the capability to record sound and/or images.

This policy applies to children, parents/carers and all staff, including our Executive (Principal / Proprietor, HR Director and Headteacher), SLT, Teachers, ALL staff, external contractors, visitors, volunteers and other individuals who work for, or provide services at the school (collectively referred to as "staff" in this policy).

Links with Other Policies

This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- iTrust
- Acceptable Use Policies (AUP)
- Character Centred PositiveBehaviour policy
- Child protection and safeguarding policy
- The Curriculum, such as: Computing, Personal Social and Health Education (PSHE) etc
- GDPR

Expectations for Safe Use of Mobile and Smart Technology Including Online Activity

Finborough School recognises that use of mobile and smart technologies is part of everyday life for many children, staff and parents/carers.

We are committed to the strong belief that good digital character as defined in our iTrust approach is at the core of safe and civil use of all technology and online activity.

Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the Finborough School community are advised to:

- Take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- Use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.

All members of the school family, students, staff and parents are expected to show good digital character as set out in our iTrust approach. The sending of abusive or inappropriate messages or content, including via personal smart devices and mobile phones is forbidden by any member of the school family; any breaches will be dealt with in line with our anti-bullying, character centred positive behaviour and child protection policies.

All members of the Finborough School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

Staff providing formal remote learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP).

School devices will be suitably protected via a passcode or pin and must only be accessed or used by members of staff.

School devices will always be used in accordance with our Staff Handbook, Acceptable Use Policy and other relevant policies.

Where staff are using school provided devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, data security, staff code of conduct and Acceptable Use Policies.
- Staff will be advised to:
 Keep mobile phones and personal devices secure during lesson time.
- Keep personal mobile phones and devices set to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- Not conduct any form of personal business using their own devices during teaching periods.
- Ensure that any content bought onto site via personal mobile phones and devices are compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting children.
- Staff will take photos or videos of children in line with our image use policy.
- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.

If a member of staff breaches these standards and expectations, action will be taken in line with our staff handbook and relevant policies.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

Students use of mobile and smart technology

Students will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.

Our iTrust approach developed in collaboration with national experts, students, staff and parents sets out a very clear detailed definition of good digital character. All students have to formally commit to having good digital character and are supported with this through regular cross school foci and as part of our ongoing character development programme.

Safe and appropriate use of mobile and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources.

Only students in year 7-13 are permitted to have a personal device / mobile phone at school.

All students in years 7-13 are encouraged to have their own laptop or tablet for learning. The school makes extensive and highly developed use of the Google platform with an associated 'enclosed' on reservation only gmail email system.

All Senior School and Sixth Form students must show sustained good digital character as set out in our iTrust approach. Cases of poor digital character will break iTrust. This will result in intervention and coaching to ensure the individual shows a sustained return to good digital character, this will be enacted in partnership with parents to ensure a 360 degree focus on the importance of good digital character.

Outside of permitted use Senior School students must keep mobile phones switched off and out of sight at ALL times during the school day.

Sixth Form students are expected to be role models of good digital character at all times.

Mobile phones or personal devices will only be used by learners during lessons or formal educational time, unless as part of an approved and directed curriculumbased activity with consent from a member of staff.

The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

Staff will only allow students to use their mobile phones or personal devices as part of an educational activity, following a risk assessment, with approval from the Leadership Team.

Finborough School expects students' personal devices and mobile phones to be kept safe and secure when on site. This means switched off, have certain functions disabled whilst on site, kept out of sight during lessons and while moving between lessons.

If a student needs to contact their parents or carers whilst on site, they will be allowed to use the office phone.

Parents are asked to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.

If a student requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with their Deputy Headteacher prior to use being permitted.

Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.

Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and their parents before use is permitted.

Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

Any concerns regarding students use of mobile technology or policy breaches will be dealt with in accordance with our existing policies and approaches, including iTrust, Anti-Bullying Policy, Safeguarding and Child Protection and Character Centred Positive Behaviour Policy.

Staff may confiscate a learner's mobile phone or device if they believe they have not met the detailed definition of good digital character set out in iTrust, this includes devices being used to contravene our child protection, behaviour or anti-bullying policy.

Students' mobile phones or devices may be searched by a member of the staff, with the consent of the student or a parent. Content may be deleted or requested to be deleted if it contravenes our policies.

Mobile phones and devices that have been confiscated will be held in a secure place and released to parents.

Appropriate restorative interventions and coaching will be implemented in line with our iTrust approach and Character Centred Positive Behaviour Policy.

Concerns regarding iTrust / policy breaches by students will be shared with parents/carers as appropriate with the expectation of 360 degree fully consistent intervention and coaching to ensure a return to sustained good digital character.

Where there is a concern that a child is at risk of harm, we will contact and respond in line with our child protection policy.

If there is suspicion that material on a student's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' use of mobile and smart technology

Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our Acceptable Use Policy and other associated policies, including child protection.

If visitors require access to mobile and smart technology, for example when working with learners as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.

Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school.

This may include undertaking appropriate risk assessments if necessary.

Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or headteacher of any breaches of our policy and iTrust approach

Policy monitoring and review

Technology evolves and changes rapidly. Finborough School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.

We will regularly monitor internet use taking place via our filtering and monitoring systems alongside comprehensive checks of devices and evaluate online safety mechanisms to ensure that this policy and our iTrust approach is consistently applied. Any issues identified will be incorporated into our action planning for further development ('better never stops').

All members of the community have been engaged in the development of our iTrust approach and will be made aware of how the school will rigorously monitor policy compliance.

Responding to policy breaches

All members of the community are informed of the need to report iTrust / policy breaches or concerns in line with existing school policies and procedures. This includes: Child Protection and Character Centred Positive Behaviour Policy

After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

We require staff, parents/carers and students to work in partnership with us to resolve issues.

All members of the school family (community) will respect confidentiality and the need to follow the official procedures for reporting concerns.

Students, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from the <u>Education People's Education</u>

<u>Safeguarding Service</u> or other agency in accordance with our Child Protection Policy.