First Tower

Digital Safeguarding

Policy

September 2021

ONLINE SAFETY POLICY

First Tower School
La Route De St Aubin
St Helier
Jersey JE2 3SD

Policy Review

This policy will be reviewed in full by the E-Safety Lead no less than annually.

The policy was last reviewed by the E-Safety Lead on 1st September 2021.

It is due for review on 1st September 2022.

Signature ……. Date ……

Head Teacher: Mrs L Linton

Signature ……. Date ……

Online Safety Lead: Mrs K Mahrer

CONTENTS	
1	**Introduction**
2	**Background**
3	**Scope of policy**
4	**Key Roles and Responsibilities**
5	**Policy and Procedure**
6	**Curriculum**
7	**Staff Training**
8	**Working in Partnership with Parents/Carers**
9	**Records, monitoring and review**
Appendix A	Acceptable Use Policy – Staff
Appendix B	Acceptable Use Policy – Volunteers
Appendix C	Acceptable Use Policy – Pupils
Appendix D	Online Safety Incident Record (staff)
Appendix E	Online Safety Incident Record (E-safety lead)
Appendix F	Declaration for Staff

FIRST TOWER SCHOOL

Digital Safeguarding Policy

1. Introduction

This policy sets out requirements for digital safeguarding in First Tower School. It covers all aspects of online and offline activities and behaviour, including the use of devices that are both school-owned and student-owned (BYOD). This document has been developed from the CYPES 'Digital Safeguarding Policy (2014) to address the school's particular digital safeguarding requirements, systems and procedures. This policy applies to policies to all stakeholders; members of staff (teaching and non-teaching), pupils/students and parents.

First Tower School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils and staff will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. Background

Schools have a duty of care under the Law to assess and prevent possible harm to children. The field of digital safeguarding, also known as e-safety, is constantly evolving with the pace of technological change and schools need to manage the attendant risks actively and in a timely manner to achieve effective digital safeguarding.

Many of the issues that arise in digital safeguarding are behavioural and their management is no different from ensuring appropriate behaviour in any other area of school life or professional activities.

First Tower will continue to request that CYPES manages the technical side of digital safeguarding so that the school will continue to be able to request advice and assistance regarding digital safeguarding incidents where required but will aim to work towards becoming more independent in the future.

3. Scope

This Policy's primary intention is to safeguard students and members of staff at First Tower and to ensure that those parties are educated to maintain their own digital safeguarding beyond the school gates.

There is a legal requirement for Jersey schools to protect children from risk of harm but there is also a moral duty for schools to protect members of staff and this additional aspect of digital safeguarding will be actively addressed alongside the protection of children.

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the school website, newsletters, social media, and events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, health and safety, home–school agreement, behaviour, and anti-bullying policies.

4. Key Roles and Responsibilities

It is the responsibility of the head teacher and the digital safeguarding lead of each school to ensure compliance with CYPES's Digital Safeguarding Policy and to meet the requirements expressed within it.

The head teacher has ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.

The named online safety lead in this school is Mrs Kathryn Mahrer

All breaches of this policy must be reported to Mrs Kathryn Mahrer

All breaches of this policy that may have put a child at risk must also be reported to the DSL (Miss Shona Mulhern)

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements. If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements

4.1 CYPES will:

- Maintain a digital safeguarding officer with overall responsibility for this area within the Department to offer schools and the Department expert advice, guidance, and recommendations. He/she will also create and update supporting documentation and resources and arrange central training.
- Monitor and review schools' digital safeguarding delivery through its digital safeguarding officer.
- Provide supported networks for hard-wired and, where applicable, mobile devices.
- Provide technical assistance for the systems that it supports via the IT Helpdesk.

- Create mechanisms whereby schools that wish to do so may take greater control over the deployment and use of approved digital safeguarding solutions.
- Continue to offer managed solutions for digital safeguarding to those schools that are not yet ready to manage their own deployments.

4.2 First Tower School will:

- Identify at least one Digital Safeguarding (E-Safety) Coordinator to manage digital safeguarding in the school and to monitor, review and develop best practice: the coordinator(s) will also be the primary contact between the school and CYPES in all matters of Digital Safeguarding (for example, requesting web-filter changes).
- Ensure that the identified individual(s) is/are given sufficient time in school to complete this role and that the identified individual(s) is/are trained to a high-level, equivalent to CEOP (Child Exploitation and Online Protection) Ambassador.
- Ensure digital safeguarding is given a suitably high priority in the school and in the school's development and improvement planning. Digital safeguarding logs, risk assessments and other documents must be made available to CYPES on request.
- Ensure all members of staff (including recently appointed staff, part-time staff, and non-teaching staff) are appropriately trained in digital safeguarding by the school's Digital Safeguarding Coordinator(s), who may draw on CYPES resources if appropriate to complement the school's own in-house expertise.
- Always safeguard the digital wellbeing of members of staff by, for example, not publishing any of their personal details (including photographs) online without consent. The school also discourages members of staff from using personal cell phones to communicate with parents or students at any time: school-owned devices should be used whenever mobile communications are needed.
- Evaluate and risk-assess new technologies to ensure that the anticipated educational benefits justify any potential digital safeguarding risks that might be identified, including by likely potential misuse of the technologies.
- Ensure that an outline of the school's approach to digital safeguarding, including responsible use of technologies and appropriate technology-based behaviour, is embedded within the home-school agreement.
- Ensure that all children are aware of their responsibilities and regularly updated about digital safeguarding issues in a meaningful and engaging manner.
- Ensure that parents and carers are aware of their responsibilities and regularly updated about digital safeguarding issues at an appropriate level.

4.3.1 School Digital Safeguarding Coordinator's Key Responsibilities

- To maintain a high level of personal training and support.
- To have a clear understanding of child protection, digital safeguarding and data protection policies and procedures.
- To report concerns to the school's Designated Safeguarding Lead and refer to the MASH team where appropriate.
- Be able to assess the e-learning benefits of any change when balanced with the associated potential digital safeguarding risks.
- Attend relevant update training and support sessions, both on-Island and elsewhere, to remain aware of the latest concerns and best practice.

- Ensure members of staff are supported with any issues they face.
- Challenge and support members of staff to develop their awareness of and teaching about digital safeguarding.

4.3.2 Monitoring Practice

The Digital Safeguarding Co-ordinator will

- Develop and keep up-to-date the school's Digital Safeguarding Policy, which must accurately reflect the requirements of CYPES's Digital Safeguarding Policy and the school's own practice.
- Ensure that signed Responsible Use Agreements (RUAs) are signed by staff, children and parents (as applicable) and that these are filed for future reference if required. Ensure there are clearly-understood measures to deter and reform inappropriate behaviour.
- Establish, monitor, and maintain a Digital Safeguarding Log, in which are recorded all issues as they arise, together with a Digital Safeguarding Risk Assessments file detailing concerns and potential new developments to show that risks have been appropriately considered and are periodically reviewed.
- Audit practice across the school and produce an action plan to improve the school's digital safeguarding provision using a self-evaluation and self-improvement framework such as SWGfL's 360º Safe (www.360safe.org.uk).
- Ensure that public communications through digital channels, including social media, are appropriately managed and consistent with all applicable policies.
- Brief staff regularly on digital safeguarding developments and new issues.
- Ensure there is an effective digital safeguarding programme in place across the school to inform and educate all stakeholders (members of staff, pupils/students, parents and others) about areas of relevance.

4.3.3 Managing Systems

- Monitor systems that are put in place to reduce and, where possible, prevent inappropriate behaviour and the accessing of unacceptable content.
- Manage and maintain different user profiles for web filtering to provide protection as appropriate and flexibility where required.
- Conduct active testing to ensure that blocked content remains inaccessible.
- Monitor the selection of all web-based services by members of staff to ensure use is consistent with those services' Terms & Conditions (including minimum age) and with all legal requirements (including Jersey Data Protection Law).
- Encourage appropriate use of file storage locations and of encrypted memory sticks for the transportation of personal data.
- Ensure procedures are in place to prevent digital safeguarding decisions from being taken by technical staff, such as IT Technicians, who may, however, implement the outcomes of those decisions as part of that procedure.
- Convey clear messages and employ workable measures to discourage users from connecting to external networks (such as 3G/4G cellphone networks and nearby, unsecured, domestic Wi-Fi networks) whilst on school premises.
- Monitor the school's online profiles and presence, including unofficial sites.
- Ensure digital safeguarding signage is displayed and regularly refreshed.

4.4 Staff Members' Key Responsibilities

- Act on all digital safeguarding issues promptly and refer these to the Digital Safeguarding Coordinator.
- Be diligent when digital safeguarding issues suggest child protection concerns: follow child protection procedures immediately in these circumstances.
- Work within the school's digital safeguarding measures and not attempt to compromise or circumvent those measures.
- Teach aspects of the digital safeguarding programme as agreed with the school and use every appropriate opportunity to raise awareness of digital safeguarding.
- Protect professional boundaries by, for example, not giving students a member of staff's mobile 'phone number; not allowing a staff network log-in to be used by a student; not becoming 'friends' with students on social networking sites.
- Be diligent in respect of data protection: use encrypted memory sticks whenever appropriate and ensure that data is always kept within authorised jurisdictions.
- Behave in a healthy, positive and professional manner towards digital technologies and when engaging in online activities.
- Select websites for school use only after reviewing their Terms & Conditions, especially regarding data protection compliance and minimum permitted age.
- Seek advice from the school's Digital Safeguarding Coordinator whenever necessary to discuss concerns, develop best practice and support students.
- Sign an appropriate Responsible Use Agreement and be aware of the responsibilities bestowed by that Agreement.

4.5 Students' Key Responsibilities

- Work within the school's digital safeguarding measures and not try to compromise or by-pass those measures.
- Know how and to whom to report anything that could improve the digital safeguarding environment and the digital/online wellbeing of students.
- Respect personal privacy and keep their own and other people's personal information private, including photographs and passwords.
- Be aware of and, where appropriate, contribute to support systems in school that encourage students to discuss any digital safeguarding concerns they may have, including peer-to-peer support and opportunities to talk to members of staff.
- Behave in a healthy and positive manner towards digital technologies and when engaging in online activities.
- Read and respect (or ask for advice or permission as appropriate) the Terms & Conditions of web services, especially regarding the minimum age that some companies set for their websites in order to protect young people from risk of harm or to comply with legal requirements.
- Sign an appropriate Responsible Use Agreement and understand what that Agreement means.

4.6 Parents' Key Responsibilities

- Discuss their school's Responsible Use Agreement with their child(ren) and explain its implications at school and at home.
- Access support systems in school and via the Internet to develop an appropriate awareness of how to protect their child(ren).
- Talk through concerns about digital safeguarding with an appropriate member of staff at their child(ren)'s school as necessary.
- Know how and to whom to report concerns to improve the digital safeguarding environment and protect their child(ren) both at school and at home.
- Work within the digital safeguarding measures that the school has in place.
- Respect digital safeguarding and data protection advice when sharing images, videos and text, especially personal information about their child(ren) via the Internet and on social networking sites.
- Respect school passwords and encourage their child(ren) never to attempt to obtain or to use another child's or an adult's password.
- Encourage their child(ren) to read and respect (or to ask for advice or permission as appropriate) the Terms & Conditions of web services, especially regarding the minimum age that some companies set for their websites in order to protect children from risk of harm or to comply with legal requirements.

5.Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff must use a school email account for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address.

Pupils should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist.

For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff and pupils should not open emails or attachments from suspect sources and should report their receipt to Mrs K Mahrer.

Users must not send emails which are offensive, embarrassing or upsetting to anyone

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from Mrs K Mahrer. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online content.

- When working with pupils searching for images should be done through Google Safe Search, Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult material that breaches the Obscene Publications Act in the UK

- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school

- Use the school's hardware and Wi-Fi facilities for running a private business

- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time.

Photographs and images of pupils are only stored on the school network. Rights of access to stored images are restricted to approved staff as determined by First Tower. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is pre-specified permission from First Tower. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils can only bring personal mobile devices/phones to school if they have had written permission from their parents. Devices must be handed in to the school secretary at the start of the school day. Under no circumstance should

pupils use their personal mobile devices/phones to take images of – any other pupil, any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with First Tower before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL the head teacher or the e-safety lead (Mrs Mahrer). Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to MASH/Social Services or the police.

6. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and should respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who

they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

7. Staff Training

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils. Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement. Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement

Guidance is provided for occasional visitors, volunteers, and parent/carer helpers

8. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides updated online safety information through the school Facebook page, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided to parents. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

9. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

Review date: September 2022 (unless interim significant policy change occurs).

Appendix A – Acceptable use policy – Staff

Acceptable use policy- First Tower School – School Owned Devices (Laptop/iPad)

As a member of First Tower School staff, you have been given an iPad/Laptop to use as a professional device to support teaching and learning in the school. This device is now your responsibility.

In order to reduce the opportunity for inappropriate use, you need to read and are asked to sign this agreement on receipt of your iPad/Laptop to acknowledge that you have been through the expectations regarding its use and that of any other devices used in school.

This agreement will be amended annually or in the light of any relevant school experiences and you will receive a copy of your signed agreement. These will be placed in staff files within school. This agreement needs to be respected by all users.

The aims of this document are:
• provide greater flexibility for e-learning on an ongoing basis;
• improve e-safety following specific incidents or awareness of new challenges;
• accommodate new devices with new capabilities.

- **User and Device**

Purpose

a. To ensure that there is no disruption to learning during periods of school closure. To enhance teaching and learning. To support staff working from home during periods of school closure.

b. It is expected that all users will act responsibly to protect their online profile and always respect the privacy of others. Facebook and other aspects of social media should be reserved for personal not professional devices. No professional devices should remain logged into personal accounts even if these are present as part of the operational system.

c. Personal devices should not be accessed for teaching and learning purposes whilst working at home during periods of school closure without permission of SLT.

d. School-owned devices are provided for exclusively educational use regardless of whether they are used at school or elsewhere (on loan).

Connectivity

School owned devices must not access ‘open networks’ or ‘public wifi’ as such networks are not filtered and their use may, therefore, give rise to e-safety incidents.

Data Protection

a. All personal data must be appropriately safeguarded on all devices and at all times. You must use strong passwords to lock the device in its entirety as well as additional blocks for specific resources e.g. password protected documents, not accessing free Wi-Fi hotspots to access school information- email, SIMS etc, where personal and sensitive data could be compromised.

b. Personally-owned devices (including storage sticks / hard drives) that are used by members of staff for professional purposes must not be used to store (either on the device or in cloud storage) any sensitive personal data that relates to other people within the school eg SEN, religion, race, sexual orientation etc.

c. All personal data that is processed in a professional capacity may be stored on web-based (cloud) services that are hosted only within the jurisdictions permitted by the school's notification (as approved by ESC, not Google) with the Office of the Jersey Data Protection Commissioner.

d. It will be the user's responsibility to ensure that third-party personal data is accessed only when the device is used in a private location e.g. the home (to avoid members of the public being able to see this information).

Safety and Virus Protection

a. School owned devices that are used professionally by members of staff must be password-protected to an appropriate degree as agreed by DfESC.

b. School-owned devices that are supplied to members of staff must be maintained in their supplied state: they must not be "jailbroken" or "rooted".

c. There is an expectation that there will be up-to-date anti-virus and other security software (such as privacy protection applications) on mobile devices/laptops. No types of devices used in school should be exempted from the need for virus/privacy protection software.

d. In the event of a school-owned device being lost, the person to whom the device was loaned must inform the school as quickly as is reasonably possible. Lost school-owned devices may be wiped-clean of all data (if provisioning / settings allows this): the assignee agrees that this may include all personal-use information too.

Rights of Inspection

a. The off-site use of all mobile devices, both home-owned and school-owned, is subject to the user granting the school a right of inspection on request.

b. Requests for inspection can be made randomly to ensure staff are following the agreed procedures, however these will only usually be made in response to a specific cause for concern or routine monitoring procedures aligned to the self- evaluation processes. Inspections will be carried-out only by designated senior members of staff. Members of staff are entitled to insist that a union representative is present throughout any inspection if they need support or are concerned. Staff should make their wishes known in advance if they have concerns.

c. Refusal to allow an inspection when one is requested may result in withdrawal of consent for the device to be used on-site/off site or of immediate termination of the applicable loan agreement in the case of a school-owned device.

d. School-owned devices must always be used in a manner that is consistent with the purposes for which they are provided: if inappropriate use is discovered during an inspection then disciplinary action may be taken.

Withdrawal of Consent

a. Devices can be used off-site only subject to acceptance of this agreement.

b. Contravening the terms of this agreement may result in withdrawal of consent to use the device and, in extreme cases, disciplinary action and/or the involvement of third-party agencies, including MASH and/or States of Jersey Police.

c. It is expected that users to whom school-owned professional devices (iPads) are loaned will bring those devices to school daily in support of teaching and learning.

d. All school-owned devices are returnable immediately on demand or on leaving the establishment for future job recruitment, even if this is within DfESC.

Reminders

All staff will be reminded of the acceptable use policy of both the Wi-Fi and school network when they log in. Individuals are beholden to this once they progress to each network, so please read these conditions and there is an expectation that staff will become familiar with them.

Staff Agreement

I acknowledge receipt of an iPad/school laptop for professional use.

I acknowledge that I have been through the school agreement and understand the aims and principles set out in this.

I agree to make every reasonable effort to preserve the life and safety of the device allocated to me.

Name:

Signed:

Date:

Appendix B Requirements for visitors, volunteers and parent/carer helpers

(Working directly with children or otherwise)

School name: First Tower School

Online safety lead: Mrs Kathryn Mahrer

DSL: Miss Shona Mulhern

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the head teacher and/or DSL

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared on line, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the head teacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Name: ……..

Date: ……

Signature: ……

- I will only use school IT equipment for activities agreed by school staff.
- If I am allowed to bring my mobile phone into school, I understand that I must hand it to my teacher when I arrive in the morning. I understand that I am not allowed to use my mobile phone on the school premises at any time. (This also includes 'smart watches' which can be used to make and receive texts/calls.
- I will not use my personal email address or other personal accounts in school
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you).

Your child's class teacher will go through the agreement with the class and ask your child to sign it. It will then be kept in school.

Any concerns or queries can be discussed with Mrs K Mahrer

Pupil agreement

Pupil name……

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature……..

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……..

Parent/carer signature……..

Date ……..……

Online safety policy guide - Summary of parent/carer responsibilities

The school provides online safety information for parents/carers, through the school website, social media, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Appendix D **Online safety incident reporting form**

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Appendix E **Online safety incident record** (e-safety lead to complete)

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to online safety Lead /DSL/ /Headteacher	
Safeguarding advice sought, please specify	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix F – Declaration for Staff

School name …First Tower School…… Academic Year …2021-2022……..

Please sign and return to …Kathryn Mahrer…. (Online Safety Lead, Deputy DSL) by Friday October 1st 2021

I, **_____<insert name>_____** have read and am familiar with the contents of the following policy and understand my role and responsibilities as set out in these document(s).:

Digital Safety Policy 2021
Mobile Phone Policy 2021
Social Media Policy 2021

I am aware that the Online Safety Lead is Mrs Kathryn Mahrer and I can discuss any concerns that I may

have with them.

I know that further guidance, together with copies of the policies mentioned above, are available in the Staff Handbook and on "Teachers' Shared"

Signed_____ Date_____