



First Tower School  
Digital Safeguarding Policy  
September 2025

**Digital Safeguarding 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 1<sup>st</sup> September 2025.

**Review date:** September 2026 (unless interim significant policy change occurs).

Signature ..... Date .....

Head Teacher: Mrs L Linton

Signature ..... Date .....

Online Safety Lead: Mrs K E Mahrer

<b>C O N T E N T S</b>	
1	<b>Introduction</b>
2	<b>Background</b>
3	<b>Scope of policy</b>
4	<b>Key Roles and Responsibilities</b>
5	<b>Policy and Procedure</b>
6	<b>Curriculum</b>
7	<b>Staff Training</b>
8	<b>Working in Partnership with Parents/Carers</b>
9	<b>Records, monitoring and review</b>
Appendix A	Acceptable Use Policy – Staff
Appendix B	Acceptable Use Policy – Visitors/Contractors
Appendix C	Acceptable Use Policy – Peripatetic Teachers, Coaches, Supply Staff
Appendix D	Letter to parents
Appendix E	Acceptable Use Policy – Rec/KS1 Pupils
Appendix F	Acceptable Use Policy – KS2 Pupils
Appendix G	Online Safety Incident Record (staff)
Appendix H	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 (2021) to address the school's particular digital safeguarding requirements, systems and procedures. This policy applies to all stakeholders; members of staff (teaching and non-teaching), pupils/students, parents and visitors.

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.

Our approach to online safety is based on addressing the following 4 categories of risk as identified in Keeping Children Safe in Education 2024:

**Content** – being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

**Contact** – being subjected to harmful online interaction with other users, for example: child-on-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

**Conduct** – online behaviour that increases the likelihood of, or causes harm, for example: making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

**Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

To meet our aims and address the risks above, we will educate pupils about online safety as part of our curriculum. For example:

- the safe use of social media, the internet and technology
- keeping personal information private
- how to recognise unacceptable behaviour online

- ensuring children know not to meet up with a person they have met online without a safe adult
- how to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they're a witness rather than a victim.

We will also:

- train staff, as part of their induction, on how to keep themselves safe online as well as children, in line with the school's online safety policy This needs to include issues for example: cyber-bullying, the risks of online radicalisation, and the roles and responsibilities around filtering and monitoring. All staff members will receive refresher training as required at least once each academic year
- educate parents/carers about online safety through letters and emails sent directly to them. We will also share clear procedures with them so they know how to raise concerns about online safety
- make sure staff are aware of any restrictions placed on them with regards to the use of their personal mobile phone and cameras,
  - *staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present*
  - *staff will not take pictures or recordings of pupils on their personal phones or cameras.*
- make all pupils, parents/carers, staff, volunteers and governors aware that they are expected to sign an agreement regarding the acceptable use of the internet in school, use of the school's ICT systems and use of their mobile and smart technology
- explain the sanctions we will use if a pupil is in breach of our policies on the acceptable use of the internet and mobile phones
- make sure all staff, pupils and parents/carers are aware that appropriate staff designated by the Headteacher or Principal, have the power to search pupil's phones, as set out in the [DfE's guidance on searching, screening and confiscation](#) if there is a concern regarding a child's safety or a crime in which case the Police will be contacted
- put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) from the school's IT systems.
- carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks faced by our school community
- provide regular safeguarding and child protection updates including online safety to all staff, at least annually, in order to continue to provide them with the relevant skills and knowledge to safeguard effectively
- review the child protection and safeguarding policy, including online safety, annually and ensure the procedures and implementation are updated and reviewed regularly.

## 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.

## 3. Scope

This Policy's primary intention is to safeguard students and members of staff at First Tower School 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/department policies and documents: Child Protection Policy, Mobile Phone Policy, Social Media Policy, GDPR, Health and Safety, Positive Relationships Policy, and Anti-bullying.

#### **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 Lead DSL (Mrs Clare Fitton)

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 forbids members of staff from using personal cell phones to communicate with parents or students at any time unless in the case of an emergency and where permission is given by the head teacher: school-owned devices should be used whenever mobile communications with parents 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 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 (e.g. CEOP Ambassador)
- 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 Acceptable Use Agreements (AUPs) 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 all issues are recorded 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 360° Safe ([www.360safe.org.uk](http://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 to protect young people from risk of harm or to comply with legal requirements.
- Sign an appropriate Acceptable Use Policy and understand what that Agreement means.

#### **4.6 Parents' Key Responsibilities**

- Discuss the school's Acceptable Use Policy 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 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. Pupils must only use their school email account to contact members of First Tower School.

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 whilst on the school premises. There may be occasions e.g. on a trip, where the only way of staff contacting a parent is by using their own device – permission must be sought from the head teacher before doing so.

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.

### **Use of mobile phones by pupils**

From the start of the academic year 2025/ 2026, Government of Jersey Schools and Colleges will not allow phone use at any time during the school day, including break and lunch times for all students up to the end of Key Stage

4. Devices accessing the internet on the school network have safe access via safeguarding software. This means that learning supported by online resources will not be impacted.

At First Tower School, we strongly discourage pupils from bringing phones to school, as there is a risk of phones being lost, damaged or used inappropriately in school. Parents can always get a message to pupils by calling the school office. We do understand that for some pupils, a phone is required and if this applies to your child please see below:

Only pupils from Year 4 upwards are allowed to bring their mobile phone to school and only once permission has been given by the Head teacher or delegate. \*excludes use of mobile phone for medical reasons e.g. monitoring blood sugar.

- Phones must be turned off at all times on school premises (including on the playground before and after school).
- Pupils must hand their phone to the school office when they arrive at school. Their phone will be kept in the school office until the end of the school day. Pupils' phones should be clearly marked with their name.
- **The school accepts no responsibility for loss or damage to mobile phones. In line with Government of Jersey guidelines, we strongly recommend pupils do not bring high value smart phones to school.**
- Whether at home or at school, please remember that mobile phones provide easy access to the Internet which is full of fantastic opportunities, but can also be a very risky place. It is important that we all work together to keep children safe. We strongly recommend that you enable parental controls on your child's phone, and talk to your child about how to stay safe online.
- Mobile phones brought to school without permission will be kept by the school office and the class teacher will contact the parents to let them know that their child has brought their phone into school without authorisation.
- Pupils are not permitted to have mobile phones during any trips, including any residential trips.

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 office at the start of the school day. ***The only exception is where the mobile device is needed to manage a medical condition e.g. Type 1 diabetes.*** 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 the school before they are brought in.

### **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 Policy as part of their induction. 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 Policy. 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 Policy. A summary of key parent/carer responsibilities will also be provided to parents. The Acceptable Use Policy 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. Incidents must also be recorded on My Concern.

## **Appendix A**

### **Acceptable Use Agreement – Staff**

You must read this agreement in conjunction with the school online safety policy. You must read, sign and submit this agreement to school where it will be kept on record. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff are aware of their responsibilities in relation to their use. All staff are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Mrs K Mahrer (Online Safety Lead) Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

### **Online conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Mrs K Mahrer (Online Safety Lead)

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

### **Social networking (please also read the school Social Media Policy)**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

### **Passwords**

All devices must be password protected (school owned and staff owned)

Do not use the same password across multiple devices/accounts

Passwords should be changed every 90 days (the school network computers should prompt users to change their password)

### **Data protection**

I will follow requirements for data protection as outlined in GDPR policy. These include:

Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely

Personal data can only be taken out of school or accessed remotely when authorised by the headteacher and an encrypted pen drive must be used.

### **Images and videos**

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

### **Use of email**

I will use my school email address for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act.

I will not use my school email addresses for personal matters or non-school business.

### **Use of personal devices**

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me because of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location.

### **Additional hardware/software**

I will not install any hardware or software on school equipment without permission of the computing lead and online safety lead.

### **Promoting online safety**

I understand that online safety is the responsibility of all staff and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, visitors, pupils or parents/carers) to the DSL or online safety lead.

### **Classroom management of internet access**

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the head teacher/deputy head.

### **User signature**

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

**Acceptable Use Policy – ALL visitors to site, including contractors (excluding parents)**

As a visitor to the school, I recognise that it is my responsibility to follow school online safety advice and that I have a responsibility to ask if I am not sure of a procedure.

This is not an exhaustive list, and all visitors are reminded that ICT use should be consistent with the school ethos and other appropriate policies.

I understand that Information Systems and ICT include not only the schools' computers, but also any personally owned equipment such as a phone or tablet and its use on social media such as Facebook or Instagram.

All school policies for Safeguarding, Child Protection, Online Safety, H&S and GDPR are available at the office if you are unfamiliar with school procedures and will be strictly adhered to throughout your time at First Tower School

Mobile phones are not allowed to be used in any sensitive areas (classrooms, cloakrooms, toilets, corridors) and instead should only be used in the staff room/office areas/meeting rooms. Mobile phones must not be used within sight or sound of children.

Cameras on personal phones or tablets MUST not be used to take pictures of children under any circumstances.

Pupils and their families have a reasonable expectation of privacy so I confirm that I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have written permission from the Head teacher.

I will not give my personal contact details such as email address, mobile phone number, IM account details to any pupil or parent in the school. Contact will always be through a school approved route. I will not arrange to video call or use a web camera with pupils unless specific permission is given.

While in the school my use of ICT and information systems will always be compatible with the ethos of the school, and if I am any doubt, I will check this with a member of staff.

Name.....

Signed..... Date .....

## **Appendix C**

### **Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers**

**School name: First Tower School**

**Online safety lead: Mrs K E Mahrer**

**Designated Safeguarding Lead (DSL): Mrs C Fitton**

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on file and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that you are aware of your responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with Mrs K E Mahrer. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy provides further detailed information as required.

#### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

#### **Online conduct**

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the online safety lead/DSL.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the head teacher.

#### **Social networking**

I understand the need to separate my professional role from my private friendships. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, parents/carers or pupils. Privileged information known because of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

### **Passwords**

I must clarify what access I may have to the internet and/or school systems whilst on the premises. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

### **Data protection**

I will follow all requirements for data protection explained to me by the school.

I must consult with the school before making any recordings, photographs and videos. Once agreed, these must only be made on a school device or an organisational device approved by the headteacher/DSL. Personal devices must not be used.

I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

### **Images and videos**

I will only upload images or videos of staff, pupils or parents/carers where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on any personal devices. These must only be made on a school device or an organisational device approved by the headteacher/DSL. Personal devices must not be used.

### **Use of Email**

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

### **Use of personal devices**

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning.

**Additional hardware/software**

I will not install any hardware or software on school equipment without permission of the head teacher or online safety lead.

**Promoting online safety**

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL or online safety lead.

**Classroom management of internet access**

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the head teacher.

**I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.**

Signature ..... Date .....

Full Name ..... (Please use block capitals)

Job Title/Role .....

Appendix D

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 equipment in school. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

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). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with the Online Safety Lead - Mrs K E Mahrer

Please return the signed sections of this form which will be kept on record at the school.

**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/carers signature.....

Date .....

**Online Safety Acceptable Use Agreement – Reception/KS1 Pupils**

These rules have been written to make sure that you stay safe when using IT equipment in school. This includes computers, laptops, iPads and Interactive White Boards. By using the IT equipment in school, you have agreed to follow these rules.

I will only use IT equipment when given permission to by an adult.

I will only open programmes/apps/activities that an adult has told me to or allowed me to use.

I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.

I will not share my password with anyone else and will never use someone else's.

I know personal information such as my full name, address and birthday should never be shared online.

I know I must never communicate with strangers online.

I am always polite when I use email and other communication tools.

**Pupil agreement**

Pupil name..... Pupil signature.....  
.....

Date.....

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.

## Appendix F

### Online Safety Acceptable Use Agreement – KS2 Pupils

These rules have been written to make sure that you stay safe when using IT equipment in school. This includes computers, laptops, iPads and Interactive White Boards. By using the IT equipment in school, you have agreed to follow these rules.

- I will only use school IT equipment for activities agreed by school staff.
- If I am given permission to bring my mobile phone into school, I understand that I must hand it in to the school office 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) – the only exception is for pupils who need to use their phone due to medical conditions.
- I will not use my personal email address or any other personal accounts in school.
- I will not sign up for any online service on a school device unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open an email attachment 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, 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 (TEAMS) should mirror that in the physical classroom.
- I will not lie about my age 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 investigate it and may need to take action.

## **Pupil agreement**

Pupil name.....

Pupil signature.....

Date.....

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.

**Appendix G**

**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):			
Full description of the incident	What, when, where, how?		

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			

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 H – Declaration for Staff**

School name ...First Tower School..... Academic Year ...2025 - 2026.....

Please sign and return to ...Kathryn Mahrer.... (Online Safety Lead, Deputy DSL)

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 2025
- Mobile Phone Policy 2025
- Social Media Policy 2025

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 \_\_\_\_\_