St Helen's School

Acceptable Use of IT Policy for Pupils

September 2022

1. Introduction

Technology plays a crucial role in teaching and learning in all sections of the School, including in the EYFS.

In the Senior School, there is a 1:1 IT device initiative whereby every student brings their own laptop, or a similar IT device to school every day for use in learning. This device must meet the school's minimum specification to be fit for learning. **Mobile phones and iPads may not be used as a pupil's 1:1 IT device.**

The 1:1 IT device scheme aims to ensure that pupils have access to tools and resources which enable them to maximise their learning wherever they are, and to better prepare them for university and the workplace. Increasing access to technology does not diminish the vital role of the teacher. On the contrary, it gives the teacher an additional set of tools to inspire greater creativity and engagement in learning.

This Acceptable Use of IT Policy for Pupils (AUP) outlines the guidelines and behaviours that pupils are expected to follow when using technology at St Helen's School. It applies to all devices used at the School, whether they are owned by the pupil or by the School. Teachers may set additional requirements for use in their classroom.

This Policy also applies to any use of technology off School premises, which affects the welfare of another member of the School community, or which brings the School into disrepute.

All use of technology at School should be for educational purposes. Pupils are expected to use good judgment and to follow the spirit of this document as well as the specifics of it: they should be safe, appropriate, careful and kind; they should NOT try to defeat or circumvent technological protection measures, but use good common sense and seek guidance where they are unsure what action to take.

It is an important part of the School's role to teach pupils how to stay safe online and what they can do if they have any problems whilst using the internet. The School is particularly alert to the need for vigilance against potential cyber-bullying and radicalisation.

2. Aims

The aims of this policy are:

2.1 to encourage all pupils, including those in the EYFS, to make good use of the educational opportunities presented by access to the internet and other electronic communication;

2.2 to safeguard and promote the welfare of pupils by limiting the risk of cyberbullying and other forms of abuse;

2.3 to minimise the risk of harm to the assets and reputation of the School;

2.4 to help pupils take responsibility for their own e-safety (i.e. limiting the risks that children and young people are exposed to when using technology);

2.5 to ensure that pupils use all technology safely and securely.

2.6 to set a framework for the acceptable use of pupils' own devices during the school day.

3. Role of technical staff

With the rapid pace of change in technology, the School recognises that blocking and barring sites alone does not provide adequate protection. St Helen's teaches all its pupils to understand why they need to behave responsibly, if they are to protect themselves. This is reinforced by the School's pastoral staff. The School's technical staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School's hardware system. They ensure that use of the internet is monitored on all IT devices in School, including pupils' own IT devices in Senior School. All email traffic, including that which is deleted by the user, is archived, and can be examined at any time.

4. Child protection and safeguarding

Internet safety is a child protection and safeguarding issue. The Deputy Head Pastoral (Mrs Neelam Varma) is the School's Designated Safeguarding Lead (DSL) and she and other key members of the Pastoral team have been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. The DSL and Deputy DSLs work closely with the Local Safeguarding Partners in promoting a culture of responsible use of technology that is consistent with the ethos of St Helen's.

The Deputy Head Pastoral and Head of Prep, together with the Acting Assistant Head Pastoral, PSHCE Co-ordinator, Director of Sixth Form and Prep Acting Assistant Head, are also responsible for the School's comprehensive PSHCE programme on e-safety. They ensure that all year groups in the School are educated at an appropriate level in the risks and the reasons why they need to behave responsibly online. It is the Deputy Head Pastoral's responsibility to oversee the handling of allegations of misuse of the internet.

In EYFS, children are supervised when using ICT and do not have access to the internet. The EYFS Safeguarding Lead (Rachael Marriott) is responsible for keeping staff informed of their duties and overseeing the implementation of this policy.

5. Misuse: Statement of policy

St Helen's School will not tolerate any illegal material being introduced and will always report illegal activity to the police and/or the Local Safeguarding Partners. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The School, in line with our Anti-Bullying Policy, will impose appropriate sanctions on any pupil who uses technology to bully, harass or abuse another pupil.

6. Involvement with parents and guardians

The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School. The School recognises that not all parents and guardians may feel equipped to protect their daughter when they use electronic equipment at home. The School therefore provides information and advice from time to time to parents (in the form of signposting to reputable resources, discussion evenings or specialist speakers) about the practical steps they can take to minimise the potential dangers to their daughters without curbing natural enthusiasm and curiosity.

7. Scope

7.1 This policy relates to the use of the full range of technology, including:

- the internet
- email
- mobile phones and smartphones / smartwatches
- school desktop / laptop computers, tablets, and any other computer
- student laptops or tablets
- devices with the capability for recording and / or storing still or moving images
- social networking, micro blogging and other interactive web sites
- instant messaging, chat rooms, blogs and message boards
- webcams, video hosting sites (such as YouTube)
- gaming sites
- Virtual Learning Environments
- SMART boards
- other photographic or electronic equipment.

7.2 This policy applies to the use of any of the above technologies, or any other technology, on School premises. It also applies to any use of technology off School premises which affects the welfare of another member of the School community, or which brings the School into disrepute. Any misuse will be dealt with in accordance with the Pupil Behaviour Policy.

8. Internet and email

8.1 The School provides internet access and an e-mail system to pupils from Years 3 to 13, to support its academic activities and to maximise the educational opportunities presented by such access.

8.2 Pupils may only access the School's network when given specific permission to do so. All pupils receive age-appropriate guidance on the use of the School's internet and email systems.

8.2.1 For their own protection and that of others, pupil use of the internet is monitored by the School, and pupil email traffic can be analysed at any point.

9. Protocols

9.1 Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible for their behaviour during classes or at break/lunchtime. Use of technology should be safe, responsible and legal. If pupils are aware of misuse by other pupils, they should talk to a teacher about it as soon as possible.

9.2 Pupils are required to read (or have explained) and comply with the following protocols as appropriate for the section of the School they are in:

9.2.1 Senior School Pupils' Protocol for using devices (Appendix 1)
9.2.2 Pupils' Mobile Phone and Smartwatch Protocol (Appendix 2)
9.2.3 Senior School ICT Acceptable Use Agreement (Appendix 3)
9.2.4 Prep School (KS2) Acceptable Use Agreement (Appendix 4)
9.2.5 Prep School (EYFS & KS1) Acceptable Use Agreement (Appendix 5)
9.2.6 Protocol for communication between staff and pupils (Appendix 6).

9.3 Any misuse of the internet will be dealt with under the School's Pupil Behaviour Policy.

10. Sanctions

10.1 Where a pupil breaches any of the School's protocols, the Governors have authorised the Headmistress to apply sanctions that are appropriate and proportionate to the breach in accordance with the School's Pupil Behaviour Policy including, in the most serious cases, expulsion. Other sanctions might include increased monitoring procedures; withdrawal of the right to access the School's internet and email facilities; detention; exclusion. Any action taken will depend on the seriousness of the offence.

10.2 Unacceptable use of electronic equipment could lead to confiscation in accordance with the protocols attached to this policy and the School's Pupil Behaviour Policy.

10.3 The School reserves the right to charge a pupil or her parents for any costs incurred to the School, or to indemnify any significant liability incurred by the School, as a result of a breach of this Policy.

11. The liability of the School

11.1 Unless negligent under the terms of this Policy, the School accepts no responsibility to the pupil or parents caused by or arising out of a pupil's use of the internet, email, or any electronic device whilst at School.

11.2 The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

12. Monitoring and review

12.1 All serious e-safety incidents will be recorded in accordance with the School's Child Protection and Safeguarding Policy.

12.2 The Deputy Head Pastoral and Head of Prep have responsibility for the implementation of this Policy. They will consider the record of e-safety incidents and new technologies and whether existing security procedures are adequate.

12.3 This policy will be reviewed by the Network Manager, Director of Digital Learning, Deputy Head Pastoral and Head of Prep on an annual basis.

Authorised by	Executive Team
Date	July 2022
Effective date of the policy	1st September 2022
Date of Next Review	July 2023

Appendix 1 – Senior School Pupils' Protocol for Using Devices

Introduction

The school network is intended for educational purposes. All activity over the network will be monitored (both over the wired and wireless network) in order to safeguard all pupils.

In accordance with Keeping Children Safe in Education (KCSIE 2022), use of devices is monitored as follows:

- For devices owned by the School (wired and wireless), all activity is monitored.
- For pupils' personal 1:1 IT learning devices, only activity which uses the School network is monitored, and this monitoring only takes place whilst the devices are on the School site.

Pupils are asked to install the InTune company portal, as directed by the School's IT administrators, to the personal IT learning device that they bring to School; this is not monitoring software but enables pupils to install apps required for teaching and learning. For pupils purchasing IT learning devices through the School, the InTune company portal will be pre-installed.

The School will never use the InTune company portal to monitor the use of personal devices; only use of the School network is monitored on pupils' personal devices and this does not require the InTune company portal to be installed.

Pupils should bring the same device to School each day. Should a pupil need to bring a different learning device to School, they must first register this device with the IT department.

The principles and rules set out below apply to all use of the internet, and to the use of email. Failure to follow this protocol will constitute a breach of discipline and will be dealt with in accordance with the School's Pupil Behaviour Policy.

When students use computers connected to the network, they must always respect these points:

- Make use of the school network via their individually authorised school network account only. Users may not share their network account access with others. Gaining access to another student's accounts, files and/or data is strictly forbidden.
- Never let anyone else know your password. If you believe that someone knows your password, you must change it immediately. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information which you are not authorised to access. If there is a problem with your passwords, please speak to your class teacher or contact the IT Dept.
- You must not load material from any external storage device brought in from outside the School onto the School's systems unless this has been authorised by the IT Manager.
- The following activities are strictly forbidden: participation in any form or illegal behaviour (e.g. credit-card fraud or electronic forgery); vandalism (any malicious attempt to harm or destroy hardware, software or data, including but not limited to the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment; transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients; bypassing the school's security; accessing a device remotely without express permission.

Access to the Internet from the School Network

The school provides its students with access to the Internet, including websites, resources, content and online tools in compliance with school policy. This access is essential to the 1:1 IT device scheme in Senior School and students will access resources through the Office 365 environment, making use of their own IT device. Access to the Internet will be restricted by our firewall in accordance with KCSIE 2022.

- Users are expected to respect web filtering as a safety precaution and should not try to disable, defeat, or circumvent it when using the Internet. If a site is blocked and a user believes it shouldn't be, the user should request access from IT Support or a teacher; the request will then be considered by the IT Manager and Deputy Head Pastoral.
- For the security of our network, users should only download files from reputable sites, and only for educational purposes. Peer-to-peer downloading (e.g downloading torrent files) is considered very high-risk and is not permitted from the school network.
- Web browsing is monitored, and activity records may be retained for up to 12 months.
- Students should remember not to post anything online that they wouldn't want parents, teachers or future colleagues or employers to see. Once something is online, it's out there – and can be shared and spread in ways that were never intended.
- Students should never share personal information relating to themselves or others, including phone number, address, birthday, or financial information over the Internet without appropriate adult permission.
- Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the School believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct. The sending, accessing, uploading, downloading or distributing offensive, profane, threatening, pornographic, obscene or sexually explicit materials, plagiarism, including accessing sites selling examination papers, book reports and other forms of student work is strictly forbidden.
- Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to e-mails. If you think, or suspect, that an attachment sent to you, or other material which you want to download, might contain a virus, you must speak to a member of the IT department before opening the attachment or downloading the material. You must not disable or uninstall any anti-virus software on the School's computers.
- Students must not plagiarise (or use as their own, without citing the original creator) content, including words or images, from the Internet. Students should not take credit for things they didn't create themselves or misrepresent themselves as an author or creator of something found online. Research conducted via the internet should be appropriately cited, giving credit to the original author. Students should recognise that communicating over the Internet does not bring anonymity and can result in associated risks and should carefully safeguard the personal information of themselves and others.
- Students should never agree to meet someone they have contacted online in real life without parental permission.
- If students see a message, comment, image, or anything else online that makes them uncomfortable or concerned for their personal safety, they should bring it to the attention of an adult (teacher or staff if at school; parent if using the device at home) immediately.
- Cyberbullying will not be tolerated. Harassing, denigrating, impersonating, tricking, excluding, and cyberstalking are all examples of cyber-bullying. Students should not send emails or post comments with the intent of scaring, insulting, hurting, or intimidating someone else. Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action. In some cases, cyberbullying can be a crime.
- Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the School.

Email

St Helen's provides students and staff with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. Email accounts should be used with care.

- Students should not send personal information by email.
- Students are expected to communicate by email in the same appropriate, safe, mindful, and courteous manner as is expected in their face-to-face communications.

- Students should not include or ask to receive anything in an email which is not appropriate to be published generally or which you believe the Headmistress and / or your parents would consider to be inappropriate for a pupil at St Helen's School.
- Use of the internet is monitored, and browsing histories and emails are archived for safeguarding purposes for up to 12 months.
- Students must not use any personal web-based e-mail accounts such as Gmail, Yahoo or Hotmail through the School's network.
- Users should not attempt to open files or follow links from unknown or untrusted origin. Users should use appropriate language and demonstrate good conduct outlined later in the policy.
- The following are strictly forbidden: spamming – sending mass or inappropriate emails (including trivial messages or jokes); use of the School's email accounts for financial or commercial gain or for any illegal activity.

Collaboration

Recognising that collaboration is essential to education, the school provides students with access to tools through Microsoft Teams that allow communication, collaboration, sharing and messaging among students. Students are expected to communicate via Microsoft Teams in the same appropriate, safe, mindful, and courteous manner as is expected in their face-to-face communications. Posts, chats, sharing and messaging may be monitored.

Student 1:1 IT Devices in Senior School

All students in Senior School bring their own IT device to school to use for learning and the School plans for all students and staff to eventually use a Microsoft Surface device. Those who join Senior School from September 2021 onwards are required to have a Microsoft Surface device and the School provides guidance to parents about this. In the transition period, students who joined the Senior School before September 2021 can make use of other personal devices as long as they fit all the essential minimum specifications set by the School. **Mobile phones or iPads/Tablets may not be used as pupils' IT devices under any circumstances.**

The fact that students bring their own IT devices to school has increased the number of opportunities for them to benefit from the use of computers and the Internet as part of their studies. However, with these opportunities comes the possibility of pupils misusing the network or the Internet and thereby causing serious harm to themselves, to other pupils or to the network.

Students must therefore adhere to all the points set out in Appendices 1, 2 and 3 of this policy when using their personal IT device in school, and in circumstances when they are joining lessons remotely from home.

- When on the School site, devices must only be connected to the School's wireless network and should not be tethered to any other network.
- Devices must be secured by a password and set to lock when not being used for 5 minutes.
- Devices must have the latest version of the following Office 365 Apps and have these configured to allow for automatic updates: Teams, Word, Excel, PowerPoint, OneDrive.
- The school's OneDrive should be synced to your device so that offline work is possible.
- Devices should have the latest operating system updates and security patches.
- Students must have the necessary software installed on their devices for teaching and learning.
- Anti-virus software must be installed and updated automatically.
- Devices must have working microphones and webcams so that remote learning can take place when needed.

- Students must have earphones or headphones, in school, that can be used with their device when needed.
- School files must be saved to the Office 365 OneDrive or shared areas to ensure that all data is backed up.
- Students are responsible for any loss of data that was not saved to the OneDrive.
- Devices should be charged every night at home and be ready to function for a full day at school.
- Devices are used in the classroom at the discretion of the teacher.
- Pupils in Middle School can use their devices at break and lunchtime for educational reasons only, in the Linkway or Library (not in tutor bases).
- Pupils in Year 10 and above can use their IT devices at break and lunchtime for educational reasons only, in the following designated areas:
  - Years 10 and 11: in tutor bases or the Library.
  - Sixth Form: in tutor bases, in Mackenzie (the Sixth Form building), or the Library.
- Devices should be kept securely in lockers or in bags when students are not in lessons.
- Whilst at school, devices may only be used for educational reasons and not for entertainment, social networking, gaming, shopping, or any other non-educational reason.

In order to aid teaching and learning, teachers may require pupils to connect to the teacher's device during lessons in school. This allows the teacher, for example, to view pupil screens, give feedback to pupils on their work, project their own or a pupil's screen on to everybody else's screen (to demonstrate learning points), and block the use of the internet or other apps which are not needed for the task in hand. Pupils would be asked to install the necessary software to their device, and they would need to actively connect to the teacher's device when asked to do so in a lesson; the teacher cannot view a pupil's screen in this way without the pupil allowing it.

Appendix 2 – Pupils' Mobile Phone Protocol

The school policy on mobile phones has not changed with the introduction of 1:1 IT devices in Senior School. Students must adhere to the following conditions if they wish to bring their phones to school:

- Mobile phones and other mobile electronic devices must be switched off (and not just on silent mode) and kept in lockers or in bags during School hours , including at break and lunch times, and between lessons. Use of such devices is only permitted during School hours with the express permission of a member of staff.
- Internet enabled wearable devices such as smartwatches are not allowed to be worn at school.
- Parents wishing to contact their children in an emergency should always telephone the School office and a message will be relayed promptly.
- Pupils in Years 7-11 must approach either the Head of Year, Acting Assistant Head Pastoral or one of the Deputy Heads to ask permission to make a phone call in the event of an emergency.
- Pupils in the Sixth Form can use their phones only in the privacy of the Mackenzie building. Phones must not be used in corridors or communal areas like the Dining Room or Reading Room.
- Pupils may not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Headmistress.
- The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated.
- Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline, whether or not the pupil is in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's Anti-Bullying and Pupil Behaviour Policies).
- The School reserves the right to confiscate a pupil's mobile electronic device for a specified period of time if the pupil is found to be in breach of this protocol. The pupil may also be prevented from bringing a mobile phone into the School temporarily or permanently and at the sole discretion of the Headmistress.

Photographs and Images

- Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- Pupils may only use cameras or any mobile electronic device with the capability for recording and / or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- Staff may request to see images stored on mobile phones and / or cameras if they have reason to believe that there may be images which contravene school rules. All pupils must allow staff access to images and must delete the images if requested to do so by staff.
- The posting of images which in the reasonable opinion of the Headmistress is considered to be offensive, on any form of social media or websites such as Youtube etc, is a serious breach of discipline and will be subject to disciplinary procedures, whatever the source of the material, irrespective of whether the image was posted using School or personal facilities and irrespective of when the image was posted.
- The School works with other agencies, including examination boards, the local authority and the police, as necessary, to ensure that the law is upheld.

Appendix 3 – Senior School Summary of Key Points

Below is a summary of the key points of this AUP for pupils in Senior School. You will be required to sign to say that you have read and understood this AUP including Appendices 1, 2 and 3, and that you agree to abide by the terms set out herein.

1. Students must have secure passwords that are not shared with any other person. If they believe someone else knows their password it should be changed immediately.
2. Never share any personal information over the internet.
3. All electronic communication should be courteous, respectful and non-inflammatory.
4. Internet usage must be for educational reasons only.
5. No external storage devices should be connected to the school network.
6. I understand that all use of the school network will be monitored, and that misuse will be dealt with in accordance with the Pupil Behaviour Policy.
7. My laptop/surface device should be fully charged each evening at home and brought to school every day.
8. A set of earphones for my device should be brought into school every day.
9. My laptop/surface device must have the necessary software installed for lessons.
10. Laptops/Surface devices should only be used on instruction by a member of staff and then for the purpose it is intended for.
11. Using chat facilities or email during lessons without instruction from the teacher is unacceptable.
12. I will share my screen with the teacher when asked to do so in a lesson.
13. Laptops/Surface devices can only be used in designated areas and at designated times when not in lessons. (See Appendix 1.) At these times, the devices are only used for work and not for streaming videos, gaming, shopping or social networking.
14. All my documents for school must be saved in my school OneDrive, which is backed up automatically.
15. It is my responsibility to keep my device safe (either in my bag or locked away in my locker) when not in use.
16. Taking or making use of photos/videos of any person without their permission is prohibited.
17. Plagiarising content of any kind is unacceptable.
18. Any form of cyberbullying is unacceptable and will result in disciplinary sanctions.
19. Mobile phones must be switched off and kept out of sight during the school day for Years 7 to 11. They can only be used with the permission of a member of staff.
20. Mobile phones and iPads/Tablets are not an acceptable 1:1 IT learning device.
21. Attempting to gain access to Internet sites by circumventing the firewall is strictly forbidden.

Appendix 4 - Prep School (KS2) ICT Acceptable Use Agreement

KEEPING SAFE: STOP, THINK, BEFORE YOU

CLICK!

These rules will keep me safe and help me to be fair to others.

- I will only use the School's computers for school work and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into School without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions, and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the School.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given me permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it, but will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Pupil Name:	Form:
Signed:	
Date:	

Appendix 5 – Prep School (EYFS & KS1) ICT Acceptable Use Agreement

ACCEPTABLE USE AGREEMENT FOR PUPILS IN EYFS AND KS1

Little St Helen's

Think before you click

S	I will only use the Internet and email with an adult.
A	I will only click on icons and links when I know they are safe.
F	I will only send friendly and polite messages.
E	If I see something I don't like on a screen, I will always tell an adult.

My Name:

My Signature:

Appendix 6 - Protocol for communication between pupils and staff

1 St. Helen's School is committed to safeguarding and promoting the welfare of children at the School. As part of our safeguarding policy we expect pupils, and where appropriate, parents, to follow this protocol on communication by mobile phone. Throughout this protocol the term mobile phone includes any mobile communication device.

Communications with Staff

2 Pupils should not use mobile phones to speak to or send messages to staff whilst in School. Telephone numbers and personal email addresses should not be exchanged or displayed.

3 Pupils should not use mobile phones to speak to or send messages to staff outside School except in specific circumstances as described below.

4 Under no circumstances should pupils use mobile phones or email to engage in communications of a personal or social nature with staff.

Emergencies

5 Where a pupil or group of pupils are involved in an emergency, they may use a mobile phone to seek assistance.

6 The leader of an educational visit will carry a mobile phone supplied by the School and, as part of the preparations for the visit, will ensure that other adults taking part in the visit are equipped with mobile phones and that relevant numbers are exchanged with pupils as required.

7 Pupils taking part in such visits may use mobile phones to speak to or send messages to staff in an emergency.

Inappropriate communications

8 If there are reasonable grounds to believe that inappropriate communications have taken place between pupils and staff, the Headmistress will require the relevant mobile phones to be produced for examination. Disciplinary procedures will apply as appropriate. Pupils may expect to have mobile phones confiscated if there has been a breach of this protocol.