FARRINGTONS
SCHOOL

ONLINE SAFETY POLICY

Author/Role	**Vanessa Suverkrop**
Date published	**September 2026**
Approving body	**SMT**
Regulatory References	**Online Safety Act 2023, Education and Inspections Act 2006, Education Act 2011, Data Protection Act 2018, Equality Act 2010, Education Act 1996, Health and Safety at Work etc. Act 1974**
Links to other policies	**Child Protection & Safeguarding Policies, Pupil Behaviour Policy, Anti-bullying Policy, Staff Code of Conduct, IT & Network Acceptable Use Policies (AUPs), Social Media & Mobile Phone Policies, Data Protection Policies, Keeping children safe in education (KCSIE)**
Date of next review	**September 2027**

Farringtons School Online Safety Policy

1. Introduction

1.1.1 Farringtons School is committed to IT services that facilitate and enhance teaching, learning and administration in the school community.

1.12 This policy provides guidance so that staff, students and other authorised users can access the school's IT resources safely, securely and within the law, and so that pupils are educated to use email, internet, mobile phones and social media appropriately. It applies to the use of school IT resources, whether on or off school premises, including laptops and mobile computing devices, software, operating systems, storage media and network accounts that provide access to local network, internet and email resources.

2. Rationale

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

2.1.2 This policy, supported by the Acceptable Use Policies (Appendix 1 & 3) for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

2.1.3 Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, tablet, digital video and camera equipment, etc) and technologies owned by pupils or staff.

2.1.4 Members of staff who breach the Farringtons School Online Safety Policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

3. The Technologies

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

3.1.2 The Internet

3.1.3 E-mail

3.1.4 Instant messaging

3.1.5 Blogs

3.1.6 Social networking sites

3.1.7 Chat Rooms

3.1.8 Gaming Sites

3.1.9 Text messaging and picture messaging

3.1.10 Video calls

3.1.11 Podcasting

3.1.12 Online communities via games consoles

3.1.13 Mobile internet devices such as Smart Phone and Tablets.

4. Whole school approach to the safe use of ICT

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

4.1.2 An effective range of technological tools which are filtered and monitored;

4.1.3 Policies and procedures, with clear roles and responsibilities;

4.1.4 A comprehensive online safety education programme for pupils, staff and parents. All staff undertake e-safety training with the Online Safety Alliance.

5. Staff Responsibilities *(also see Online Safety Monitoring Policy in Appendix 2)*

5.1.1 Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of staff, aims to embed safe practices into the culture of the school. The Head ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis.

5.1.2 The Designated Safeguarding Lead has overall responsibility for the monitoring of online safety (See online safety monitoring policy) they will work closely with the Data Manager and IT Network Manager in ensuring that online safety is maintained.

5.1.3 The Designated Safeguarding Lead ensures that they keep up to date with online safety issues and guidance provided from such organisations as The Child Exploitation

and Online Protection (CEOP). The Designated Safeguarding Lead also ensures that the Head, Senior Management and Governors are updated as necessary.

6. Staff awareness

6.1.1 All staff receive regular information and training on online safety issues in the form of in house training within INSET and online refresher courses through platforms like iHASCO.

6.1.2 New staff receive information on the school's acceptable use policy (AUP) as part of their induction.

6.1.3 All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

6.1.4 All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.

6.1.5 Online safety concerns are reported directly to the School's safeguarding team.

6.1.6 All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies at Farringtons.

7. Internet

7.1.1 Farringtons School internet access is 'filtered' by onsite filtering software, which helps minimise the chances of pupils encountering undesirable material.

7.1.2 Staff, pupils and visitors have access to the internet through the school's fixed and mobile internet technology.

7.1.3 Staff should email school related information using their school email address and not personal accounts.

7.1.4 Staff will preview any websites before recommending them to pupils.

7.1.5 If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.

7.1.6 If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to IT Network manager. This will be escalated to the Designated Safeguarding Lead, and the website blocked by the IT Network Manager.

7.1.7 Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.

7.1.8 Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher and then this will be reported to the IT Network Manager

7.1.9 Pupils are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.

7.1.10 Pupils are taught the rules of etiquette in email and are expected to follow them.

7.1.11 No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

7.1.12 Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the School's Behaviour Policy.

7.1.13 Pupils will be asked to sign to the Acceptable Use Policy as part of the joining paper work. Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.

With specific relation to staff:

8. Passwords

8.1.1 The school recommends that staff use a strong password for their IT accounts (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers and symbols).

8.1.2 Passwords should not be written down.

8.1.3 Passwords should not be shared with other children or staff.

9. Mobile technology (laptops, iPads, netbooks, etc):

9.1.1 Mobile technology for pupil use, such as laptops or tablets are stored within the trolley safe within the designated classrooms. Access is available to pupils when staff lessons require the use of the laptops or tablets.

9.1.2 Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.

9.1.3 When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

9.1.4 With the exception of potential 'two factor authentication' notifications which should be rare on site, no personal mobile phone devices belonging to staff are to be used during lessons at school. These are to be used during break times only and kept on silent. If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should only be used in accordance with the School Rules, and will remain the responsibility of the child in case of loss or damage. Any children not following these rules will be dealt with using the School's Behaviour Policy.

10. General Data Protection Regulations (GDPR) and data storage

10.1.1 Staff must be aware of their responsibilities to ensure that confidential information and data is kept secure. Staff are expected to save all data relating to their work in their staff home documents area, school shared drives or their school OneDrive.

10.1.2 There are considerable legal and financial consequences involved in not complying with the GDPR legislation so it is an expectation of staff at Farringtons that they will follow these instructions:

- Always lock your account when leaving your desk/PC/laptop/tablet etc.
- Always ensure paper documents, which identify individuals (even if just by name), are locked away in a filing cabinet/desk drawer – or destroyed (safely shredded in school) if no longer required.
- Staff are prohibited from sending staff or student data outside of the school by any means without the express permission of the Head and Data Manager.
- You should not save or transfer any personally identifiable data to USB memory sticks/hard drives or other such storage devices unless these have been authorised and are encrypted.
- You should not send personal data to personal email accounts, personal cloud based storage areas or otherwise. Please make use of Office 365 through your school account which can be accessed securely via our network.
- Ensure that if you use a personal device to check your school email account, this is adequately protected with passwords and finger print or facial recognition software.

- If you suspect or become aware of a data breach, you must notify the Bursar and Data Manager as soon as you become aware of this. A data breech can be as simple as sending an email to the wrong person, losing your personal mobile device which has access to your school email account etc.

10.1.3 This list summarises the key points from the GDPR legislation but does not cover all eventualities. If there specific circumstances not detailed above, staff should contact the Data Manager or the Bursar for advice on how to proceed.

11. Social Networking Sites

11.1.1 Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.

11.1.2 Under no circumstances should school pupils or parents, past or present, be added as friends (or equivalent), unless known to you as a friend or relative prior to your appointment, as your role in school requires a high degree of professionalism and confidentiality.

11.1.3 Any communications or content you publish that causes damage to the School, or any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Disciplinary Policies apply.

11.1.4 Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

11.1.5 Any communications made in a professional capacity with other members of the staffing body through social media must not either knowingly or recklessly:

- Place a child or young person or member of staff at risk of harm;
- Bring the School into disrepute;
- Breach confidentiality;
- Breach copyright;

11.1.10 Staff must not breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- Using social media to bully another individual; or
- Posting images that are discriminatory or offensive or links to such content.

11.1.14 The School reserves the right to monitor staff and pupils internet usage. The School considers that valid reasons for checking internet usage include concerns that social media / internet sites have been accessed in breach of this Policy.

12. Digital images

12.1.1 Use only digital cameras and video cameras provided by the school and under no circumstances use personal equipment such as digital cameras or mobile phones to store images of children.

12.1.2 When using children's images for any school activity, they should not be identified by their name unless parental permission has been given in writing (See *Photography Policy*)

13. Providing a comprehensive online safety education to pupils and parents

13.1.1 All staff working with children must share a collective responsibility to provide online safety education to pupils and to promote online safety in their own actions.

13.1.2 Formally, online safety education is provided by the objectives contained in the ICT schemes of work for every area of work for each year group. Even if online safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the ICT curriculum.

13.1.3 Informally, a talking culture is encouraged in classrooms which allows online safety issues to be addressed as and when they arise, particularly in lessons like Wellbeing.

13.1.4 Where needed the Designated Safeguarding Lead will provide an assembly on the online safety risks.

13.1.5 Staff will ensure children know to report abuse to any member of staff who will escalate the concern to the Designated Safeguarding Lead.

13.1.6 When children use school computers, staff should make sure children are fully aware of the Student Acceptable Use Policy. (See Appendix 1)

Appendix 1:

Pupil Acceptable Use Policy

FARRINGTONS SCHOOL

Information & Communication Technology
Student Acceptable Use Policy

This code of conduct applies at all times, in and out of school hours, whilst using school equipment. Please read it carefully.

You should:

- ✓ Only access sites which are appropriate for use in school.
- ✓ Be aware that your actions on the Internet can be seen by others
- ✓ Be aware that information on an Internet web site may be inaccurate or biased. Try to verify the information using other sources, if possible, before using it.
- ✓ Be careful of what you say to others and how you say it.
- ✓ Respect copyright and trademarks. You cannot use the words or pictures that you see on an Internet site without giving credit to the person that owns the site.
- ✓ Check with a teacher before opening email attachments or completing online questionnaires or subscription forms.

You should not:

- X Give your password to anyone else or allow them to use your account.
- X Download games or other programs from the internet or elsewhere
- X Use social networking sites or unauthorised web-based email services
- X Send, access or display offensive messages or pictures
- X Use or send bad language
- X Waste time on the computer doing things that are not related to your work in school.
- X Give your name, address, telephone number or any other personal information about yourself or others to anyone you write to.
- X Intentionally cause damage to the computer system or equipment.

Please note:

- Student areas on the school network will be closely monitored and staff may review your files and communications to maintain system integrity.
- Failure to follow the code will result in loss of access and further disciplinary action may be taken if appropriate. If applicable, external agencies may be involved: certain activities may constitute a criminal offence.
- Students should always read the Acceptable User Policy code displayed at log in.

General Usage

1. You are responsible for safeguarding your password for the system. For reasons of security, your individual password should not be printed.
2. Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so.
3. The School has software and systems in place that monitor and record all Internet usage
4. Our IT team will review Internet activity and analyse usage patterns, and they may choose to publicise this data to ensure that School Internet resources are devoted to curriculum- and School-related activities.
5. The display of any kind of sexually explicit image or document on any School system is in violation of our policies. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
6. Users shall not perform any other inappropriate uses identified by the network administrators.
7. Use of your own equipment is permitted so long as you adhere to the rules defined in this document. Any disregard to these rules will result in your device being blocked from accessing the school network.
8. You must use the Farringtons Cloud system if you wish to ensure your work is backed up. If you save your work locally to your device then we cannot guarantee any recovery of work.

Information & Communication Technology
Student Acceptable Use Policy

E-mail Usage

1. Users should not make derogatory remarks in e-mails about any other person. Any written derogatory remark may result in your account being locked.
2. Try not to create e-mail congestion by sending trivial messages or unnecessarily copying e-mails. Users should regularly delete unnecessary e-mails to prevent over-burdening the system.
3. By sending e-mails on the School's system, you are consenting to the processing of any personal data contained in that e-mail and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If you do not wish the School to process such data you should communicate it by other means.

Internet Usage

1. First and foremost, the Internet for this School is a work and curriculum tool, provided to you at significant cost. That means we expect you to use your Internet access primarily for work- and curriculum-related purposes, i.e., to research relevant topics, to obtain information.

2. Unnecessary or unauthorised Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources; inappropriate Internet usage may also gain negative publicity for the School and expose the organisation to significant liabilities.

3. While our direct connection to the Internet offers a cornucopia of potential benefits, it also opens the door to some significant risks to our data and systems if we do not secure the IT Network appropriately.

4. This School's Internet facilities and computing resources must not be used to violate the laws and regulations of the UK or any other nation.

5. Any software or files downloaded via the Internet into the School network become the property of the School. Any such files or software may be used only in ways that are consistent with their licenses or copyrights and in accordance with School policy.

6. No user may use School Internet facilities to download or distribute pirated software or data, nor to propagate any virus, worm, Trojan horse, or trap-door program code.

7. No user may use the Schools Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

8. Users with Internet access may download only software with direct curriculum use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license and in previous agreement with IT Department.

9. Users may not use School Internet facilities to download entertainment software or games or to play games against opponents over the Internet. Images and videos must not be downloaded unless there is an express work- or curriculum-related need.

Acceptance

I have agreed to the above and agree for my account to be activated with the above restrictions and acceptable use regulations.

Name of Pupil _____ Form: _____

Signed (Pupil): _____ Date: _____

Signed (Parent/Guardian): _____ Date: _____

Appendix 2:
Farringtons School Online Safety Monitoring Policy

1. Introduction

1.1.1 Farringtons School uses Smoothwall educational software to monitor the online activity of our students and staff and their use of the School's I.T. Network.

1.1.2 There are four types of online moderation that the School uses to aid with online safety monitoring:

1. **Pre-monitoring;** Material reviewed for suitability prior to being visible to others
2. **Post-monitoring;** Material reviewed after it is visible. Time delay may be variable, although real time monitoring and alerting is possible through the Smoothwall software used within the School.
3. **Sample monitoring;** Moderator "patrols" a cyber (or physical) space or samples a selection of content usually as student work is work is being completed.
4. **Reactive monitoring;** Occurs after a request is made for intervention

1.1.3 In addition to online moderation, Smoothwall enables work completed by students and staff within the School I.T. Network to be monitored as well. The software is able to flag vocabulary and content that may be associated with safeguarding themes.

2. Student monitoring

2.1.1 **Designated Safeguarding Lead Tasks**

2.1.2 The following are completed on a weekly basis as a minimum:

- Review and react to immediate high priority Smoothwall alerts.
- Review Smoothwall weekly reports detailing attempted suspicious search queries and blocked websites.
- Review trends / patterns of behaviour based on Smoothwall data and proactively investigate as required.

2.1.3 The Designated Safeguarding Lead and the Data Manager will meet regularly and at least every half term as a minimum to ensure Smoothwall is responding appropriately to meet the needs of the School.

2.1.3 **Staff Responsibility**

2.1.4 All staff have a professional responsibility to report any online activity that they feel is inappropriate or raises specific safeguarding concerns.

2.1.5 Safeguarding concerns should always be reported to Mr Simon Smith, the Designated Safeguarding Lead and recorded through My Concern (see Appendix 1).

2.1.6 It may also be appropriate to contact Mrs Vanessa Suverkrop, the Data Manager, who also liaises with R.M. Education our I.T. network partners, if a particular website is being accessed and needs to be blocked, or there is an issue within the network that needs resolving to keep students safe.

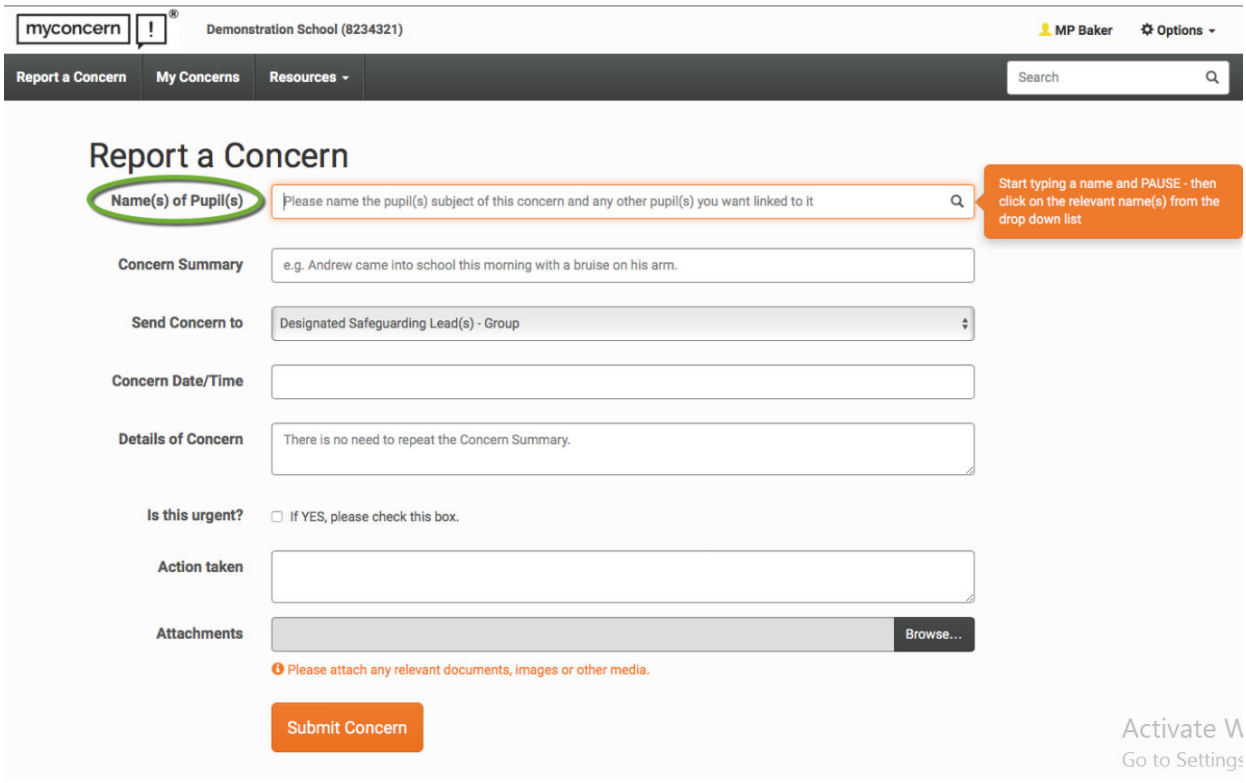
3. Website blocking and unblocking

3.1.1 Smoothwall allows for some changes to be made to the definitions with which it recognises the content of websites. Requests for access to blocked websites, usually for teachers to use in their lesson delivery, can be made using the IT Help desk but maintaining our school-wide safeguarding responsibilities and the integrity of the School I.T. Network as a whole will always take priority.

Appendix 2.1

MyConcern can be accessed at https://myconcern.education.

Staff should login and raise a concern using the Report a Concern icon.



Appendix 3
Staff Acceptable Use Policy

Guidelines for Staff

The School has provided computers for use by staff as an important tool for teaching, learning, and administration of the School. Use of School computers by staff is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the IT Network Manager in the first instance.

All members of staff have a responsibility to use the School's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the School's computer system may result in disciplinary action (including possible dismissal), and civil and/or criminal liability.

Please note that use of the School network is intended to be as permissive and flexible as possible under current UK legislation. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the School and staff, to safeguard the reputation of the School, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the School recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. While the School neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the School.

Computer Security and Data Protection

- You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, you must not disclose your password to anyone, including IT Support staff. If you do so, you will be required to change your password immediately.
- You must not allow a pupil to have individual use of a staff account under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.

- You must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the School.
- You must not transmit any sensitive or personal information about staff or students via email
- When publishing or transmitting non-sensitive material outside of the School, you must take steps to protect the identity of any pupil whose parents have requested this.
- If you use a personal computer at home for work purposes, you must ensure that any School-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.
- You must not make your own backup of data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the School) or a personal computer.
- You must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment, other than staff laptops, taken offsite is not routinely insured by the School. If you take any School computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.

Telephony

The school operates a "hot desk" telephone system and every member of staff is issued with their own "Extension" and "PIN". Key members of staff will also be issued with a mobile phone, which this policy also applies to.

Telephones must not be used for personal telephone calls and only for business related calls – all phone calls in and out are logged by our logging software and by the service provider, if a mobile.

Most Mobile Phones are on "contract" and as such – fair limits, fair use and caps apply.

Personal Use

The School recognises that occasional personal use of the Schools computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use

- must comply with all other conditions of this AUP as they apply to non-personal use, and all other School policies regarding staff conduct;
- must not interfere in any way with your other duties or those of any other member of staff;
- must not have any undue effect on the performance of the computer system; and
- must not be for any commercial or political purpose or gain unless explicitly authorised by the School.
- Personal use is permitted at the discretion of the School and can be limited or revoked at any time.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by the Schools normal rules on electrical safety testing.
- You must not connect personal computer equipment to School computer equipment without prior approval from IT Support staff in writing, with the exception of storage devices such as USB memory sticks.
- If you keep files on a personal storage device (such as a USB memory stick), you must ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the School computer system.
- You must not use your personal device for the purposes of hacking or modify the school IT systems.
- You must use the Farringtons Cloud system if you wish to ensure your work is backed up. If you save your work locally to your device then we cannot guarantee any recovery of work.

Conduct

- You must at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;

    - Making ethnic, sexual-preference, or gender-related slurs or jokes.

- You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You must not intentionally damage, disable, or otherwise harm the operation of computers.
- You must make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive storage of unnecessary files on the network storage areas;
    - Use of computer printers to produce class sets of materials, instead of using photocopiers.
- You should avoid eating or drinking around computer equipment.

Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook, Twitter, LinkedIn or Instagram, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You must not add a pupil to your 'friends list' (or similar).
- You must ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- You should avoid contacting any pupil privately via a social networking website, even for School-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the School – even if their online activities are entirely unrelated to the School.

- Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the School.
- You should not post any material online that can be clearly linked to the School that may damage the School's reputation.

- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the School. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You must be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You must not purchase goods or services on behalf of the School via e-mail without proper authorisation.
- All School e-mail you send should have a signature containing your name, job title and the name of the School.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you must not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the School.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The School will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of Pupil Use

- Pupils must be supervised at all times when using School computer equipment. When arranging use of computer facilities for pupils, you must ensure supervision is available.

- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Privacy

- Use of the School computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the School to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the School does keep a complete record of sites visited on the Internet by both pupils and staff and logs of all email messages. Usernames and passwords used on those sites are NOT monitored or recorded.
- You should avoid storing sensitive personal information on the School computer system that is unrelated to School activities (such as personal passwords, photographs, or financial information).
- The School may also use measures to audit use of computer systems for performance and diagnostic purposes.
- Use of the School computer system indicates your consent to the above described monitoring taking place.

Confidentiality and Copyright

- Respect the work and ownership rights of people outside the School, as well as other staff or pupils.
- You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the School computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You must consult a member of IT Support staff before placing any order of computer hardware or software, any computer peripheral or obtaining and using any software you believe to be free. This is to check that the intended use by the School is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the School's systems.

- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of the School or capable of being used or adapted for use within the School shall be immediately disclosed to the School and shall to the extent permitted by law belong to and be the absolute property of the School.
- By storing or creating any personal documents or files on the School computer system, you grant the School a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the School sees fit.

Reporting Problems with the Computer System

It is the job of the IT Network Manager to ensure that the School computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of IT Support staff as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem must be reported via the online service request system.
- If you suspect your computer has been affected by a virus or other malware, you must report this to a member of IT Support staff immediately.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform a member of the IT Support staff, or the Head, of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within School that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the School computer system.

Reports should be made either via email or the online services request system. All reports will be treated confidentially.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

"Sensitive personal information" is defined as information about an individual that is protected by law under the Data Protection Act 1998. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive. Further information can be found in the School's Data Protection Policy.

Staff AUP Acceptance

I have read and understood the Farringtons School acceptable use policy for staff and agree to abide by its terms and conditions.

Signed: _____

Name: _____

Date: _____

Appendix 4
Acceptable Use Policy (AUP) Class Cameras (Refurbished iPhone XRs)

The refurbished iPhone XRs are designated school devices for the sole purpose of capturing photographs and videos to support teaching, learning, school documentation, and approved communication with parents. Their introduction is intended to improve the quality of school imagery while reducing reliance on personal devices and strengthening safeguarding and data protection controls.

These devices are not communication tools and are not general-purpose digital devices. They exist only as air-gapped cameras for school use.

Device Status and Configuration

All iPhone XRs must be configured as air-gapped devices. This means they must:

- Contain no SIM card.
- Never connect to Wi-Fi, mobile data, or any external network.
- Have Wi-Fi, Bluetooth, AirDrop, and Personal Hotspot permanently disabled.
- Not be signed into any Apple ID.
- Not be paired with any other device.
- Have no additional applications installed.

The default camera function is the only permitted function of the device.

Any attempt to connect a device to the internet or enable communication features must be reported immediately to the Head of Prep School or the nominated safeguarding lead.

Use Restriction (Absolute)

These devices are strictly photography and video capture tools.

They may only be used to:

- Take appropriate photographs or videos for school-related purposes.
- Record learning activities, trips, events, displays, and achievements.
- Support school communications where parental consent and school policy allow.

They must never be used for:

- Any form of communication, including calls, messages, email, or social media.
- Browsing the internet.
- Audio-only recording.
- File sharing or transfer via AirDrop or Bluetooth.
- Personal photography or video recording.
- Any non-school-related activity.

In summary:
No communication.
No connectivity.
No additional applications.
No secondary use.
Photography and video only, for appropriate school purposes only.

Storage and Physical Security

- Devices must be stored on site when not in use.
- Devices must be kept in locked drawers or cupboards in designated secure locations.
- Access is limited to authorised staff only.
- Devices may only be taken off site for approved school trips or visits and must be returned to secure storage immediately afterwards.
- Devices must never be taken home or used for personal purposes.

Passcode Security

- Each device must be protected by a passcode set by the Head of Prep School or a nominated senior member of staff.
- The passcode must be recorded securely alongside the central device register.
- Passcodes must not be shared beyond the specific classroom or authorised staff group using that device.
- Passcodes must not be written down informally, photographed, or stored digitally outside the secure register.
- Any suspected compromise of a passcode must be reported immediately and the passcode reset.

Photo and Video Transfer

- All photos and videos must be transferred to the school's approved, secure systems as soon as practicable.
- Transfer must be completed using a local, on-site physical cable connection only.
- Wireless transfer methods are strictly prohibited, including:
    - AirDrop
    - Bluetooth
    - Cloud services
    - Email
    - Any internet-based platform

Transfer may only be made to school-managed devices or storage systems that comply with safeguarding and data protection requirements.

Deletion Protocol

- Once transfer has been confirmed, all photos and videos must be deleted immediately from the device.
- Devices must never be used as long-term storage.
- No images should remain on any device longer than is strictly necessary for secure transfer.

Termly Review

- A full review of each device must take place at least once per term.
- During this review:
    - Any remaining images must be transferred or deleted.
    - Devices must be confirmed as empty of historic content.
    - Compliance with this policy must be recorded.

Register and Accountability

A central register must be maintained by the Head of Prep School or a nominated senior member of staff. The register must include:

- Device model and serial number.
- Assigned storage location.
- Passcode storage confirmation.
- Staff authorised to use the device.

- Dates of issue and return.
- Termly audit completion.

This register provides traceability, safeguarding assurance, and accountability.

Safeguarding and Data Protection
All use must comply with:

- The school's safeguarding policy.
- The school's photography and image-use policy.
- UK data protection legislation.

Staff must ensure:

- Images are taken respectfully and appropriately.
- Pupil dignity and privacy are preserved at all times.
- Consent requirements are adhered to.
- Images are never shared informally or stored outside approved systems.

Any loss, damage, misuse, or safeguarding concern must be reported immediately to the Head of Prep School or DSL.

Monitoring and Compliance

- Compliance with this AUP will be checked regularly.
- Any breach may result in:
    - Immediate withdrawal of device access.
    - Review under staff conduct procedures.
    - Further safeguarding or disciplinary action where necessary.