FURZE PLATT
SENIOR SCHOOL

Internet Safety Policy

1. Introduction

The purpose of internet use at school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school’s management information and business administration systems.

The internet is an essential element in 21st century life for education, business and social interaction. The school aims to provide students with quality internet access as part of their learning experience by using online tools for teaching, learning and assessment.

The school embraces its role in promoting on-line safety and in safeguarding students’ welfare when using information and communication technology. We aim to educate our students so that they are aware of how to use the Internet safely. We deploy a range of hardware and software systems to reduce online line risks and have in place a set of procedures which enable staff and students to use the Internet safely and responsibly.

2. Internet education

Students are encouraged to develop skills which allow them to become discriminating and productive internet users. The skill development opportunities are incorporated into programmes of study ICT and regularly reinforced in other subject areas.

- Internet access is planned to enrich and extend learning activities.
- Staff guide students in online activities that support the learning outcomes planned for the students’ taking into account their age and maturity.
- Students are educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.
- Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students are taught to acknowledge the source of information and to respect copyright when using internet material in their own work.
- The school encourages practices which ensure that the use of internet derived materials by staff and by students complies with copyright law.
- Online safety is a key focus of the internet education provided by the school. Opportunities to discuss and explore these issues are provided within the ICT, PSHE, Assembly and tutorial programmes.
- Students are taught how to keep themselves safe whilst online and how to report activities which present a risk to themselves and others.

3. Use of email

- Students may only use email accounts provided by the school.
- Access in school to external personal email accounts is blocked.
- Email sent to an external organisation by staff must be written carefully using the appropriate professional tone and language.
- In the school context, emails will not be considered private and the school reserves the right to monitor emails of both staff and students. The school is mindful of the need to balance the need to maintain the safety of students and the preservation of privacy.
- The email addresses of key staff will be provided to parents.
- Staff may respond directly to parental communication via email but must regard such communication as official and they should be written in an appropriately formal and professional style.

- The school uses ParentMail, a proprietary system, to facilitate bulk-mail to parents. This service is managed remotely. Parents may subscribe and unsubscribe themselves from this service. The school will not send unsolicited mail to parents using email addresses provided to the school for other purposes.
- Online communication between staff and students will, for the protection of both parties, be through the approved school systems where such communication is easily monitored and tracked. Private email addresses must not be shared between staff and students.
- Staff private telephone numbers must not be shared with students. School mobile telephones are provided for staff on school trips so that students can make telephone contact in an emergency.
- Staff must be particularly mindful of the need to maintain an appropriate and professional tone in all electronic communication with students.
- Should a member of staff have reason to feel professionally uncomfortable or compromised by the tone or content of an electronic communication then this must be reported to their line manager at the earliest possible opportunity.
- Students are educated to report any undesirable or abusive electronic communication to a member of staff whatever the source.
- Teachers' professional obligations with regard to internet use, social media and email are components of the annual whole staff child protection training.
- Staff must exercise care when sharing personal information publicly online, and be conversant with the privacy settings of any social networking service used so as to minimise risk.
- Staff must take care to ensure any views expressed publically online do not compromise their professional integrity nor reflect poorly on the school.

4. The school website

The school website is a valuable means of publicising the school and providing useful information to parents and the community. Due to the public nature of the internet the following protocol is used to ensure appropriate content:

- The point of contact on the website is the school address, school email and telephone numbers. Staff or students' home information will not be published.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website. This is achieved through the annual information check.
- The Headteacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.
- Guidance and training will be provided to those staff who have permissions to edit site content or post on the school's social networking sites.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- The materials published on the website will include the items specified in the Governors' School Publications policy.

5. Internet access

- Internet access is provided for all staff and students.
- A copy of this Policy is posted on the school website.
- Parental permission for students to be given internet access is confirmed annually through a data collection and confirmation exercise.

6. Internet content and other electronic media

The school recognises its responsibilities in protecting students from exposure to unsuitable material. The school also recognises the requirement to exercise vigilance and its duty to prevent students being radicalised and drawn into terrorism as part of the PREVENT duty. A number of systems are in place to minimise the risk of students accessing unsuitable materials.

- The school takes reasonable precautions to ensure that users access only appropriate material. However, it is not possible to guarantee that unsuitable material will never appear on the school computers. The school cannot accept liability for the material accessed, or any consequences of internet access.
- Methods to identify, assess and minimise risks are reviewed regularly. The school will utilise a proprietary web filtering system and augment this by other safeguards as appropriate. Various levels of web filtering are in place. As students progress through the school into the sixth form, filtering levels are adjusted to reflect the students' maturity and their broader research needs. Unfiltered access is available for IT support staff only whose work in testing on line services demands this facility.
- Where a site has been blocked by our default filtering policies, staff may request that the site is unblocked for educational or professional development reasons. Such request are scrutinised by the Headteacher or nominee to ensure that the site presents no significant risk to students.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the network manager.
- Rules for internet access are posted near all fixed computer systems.
- Students and staff are informed that Internet use is monitored.
- A module on responsible and safe internet use is included in the ICT programme and the topic is covered in PSHE and the tutorial programme.
- All staff must accept the terms of the 'Responsible internet Use' statement before using any Internet resource in school (see Appendix.)
- Staff are made aware that internet traffic can be monitored and traced to the individual user. Professional conduct is essential.
- The monitoring of staff Internet and email use will only be initiated by the Headteacher and supervised by a member of the Senior Leadership Team.
- The 'YouTube' video sharing site is available for staff use only. Videos from the site will be downloaded or linked to through the school's intranet. The 'YouTube' website will not be used in the presence of students as the results of searches can display materials which could be inappropriate.
- Staff will ensure that any written, audio or visual material used is appropriate for the children to whom it is displayed. Staff will use caution in this matter and confer with a senior colleague for guidance as necessary.

- Staff should only capture images of students for school use. When a member of staff's personal device is used to take the photograph or record video, the images should be erased from the device or storage media as soon as is practical.

7. Online communities, newsgroups and chats

The school recognises its responsibilities in protecting students from communications with unauthorised individuals.

- Social media sites, public and unregulated newsgroups, chat rooms, blogs and online communities can be of educational use. These present an unacceptably high risk to the safety of younger students and so these sites are blocked for all students below Year 12. Some selected sites are unblocked for 6th formers.
- The use of school provided discussion forums is allowed but will be closely monitored.
- Internet access via students' personal mobile devices cannot be regulated. There is, however, a campus wide ban on the sight and sound of handheld electronic devices which will help to minimise risks on campus.

8. Emergent technologies

- Senior staff will maintain an up to date knowledge of emergent internet technologies and their potential for delivering educational or institutional benefits. New technologies will only be implemented after a thorough risk assessment.

9. Misuse of the school computer system and internet

- Misuse of the school's computer system by students will be dealt with in accordance with the school's behaviour policy framework.
- Misuse of the school's computer systems by staff will be dealt with in accordance with the school's Staff Disciplinary Policy. Any complaint about staff misuse must be referred to the Headteacher.
- When appropriate, the school's Designated Senior Person (DSP) for child protection will be involved in accordance with the Child Protection and Safeguarding Policy.

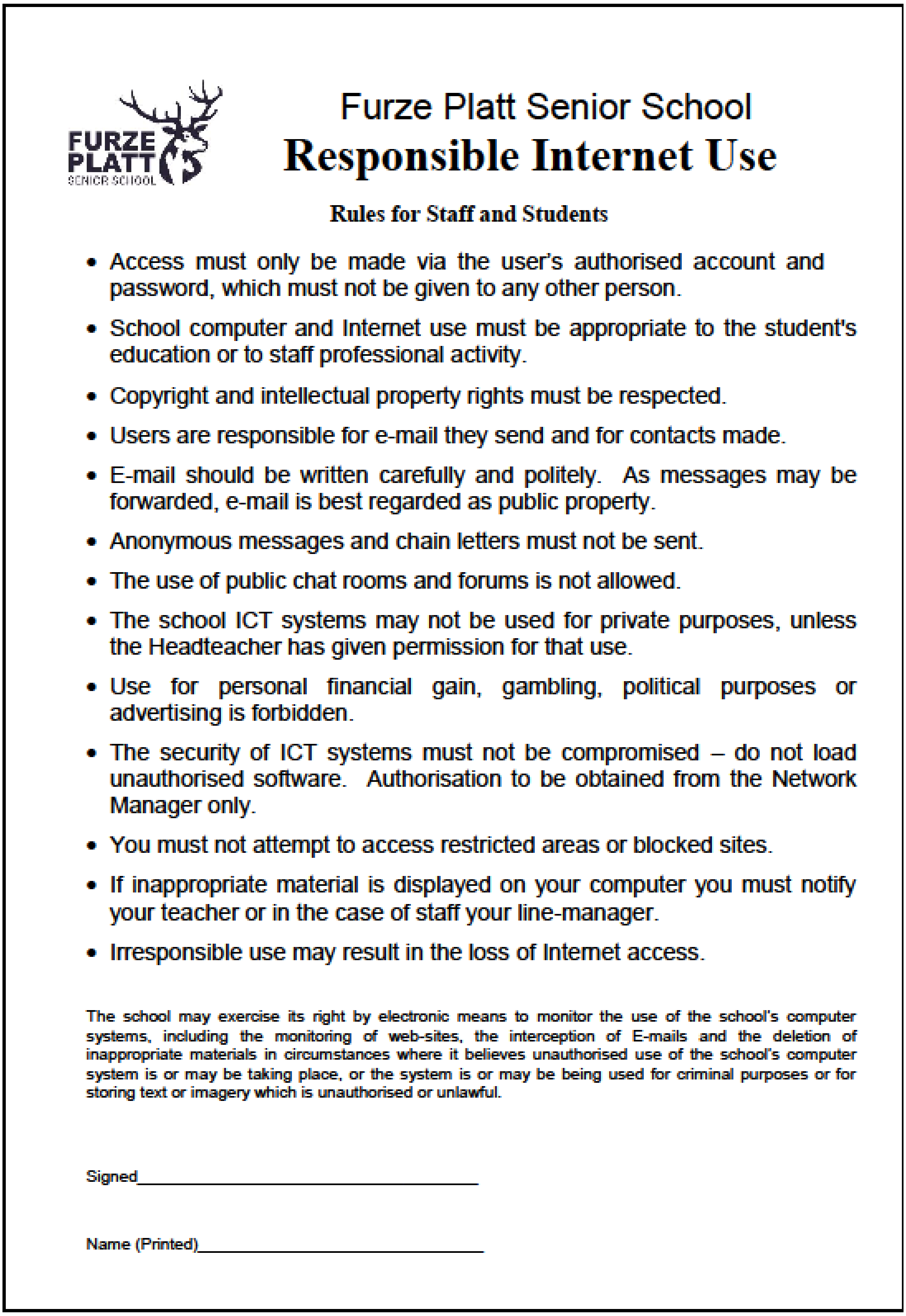
10. Monitoring and evaluation

The day to day implementation of this Policy will be monitored by the Senior Leadership Team member responsible for ICT developments. Monitoring activities will include:-

- fortnightly meetings with the Network Manager;
- fortnightly meetings with the Head of ICT.

The review and evaluation of this Policy is the responsibility of the Governors' Pupils and Parents Committee.

APPENDIX



FURZE PLATT SENIOR SCHOOL

Furze Platt Senior School

Responsible Internet Use

Rules for Staff and Students

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- Users are responsible for e-mail they send and for contacts made.
- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
- Anonymous messages and chain letters must not be sent.
- The use of public chat rooms and forums is not allowed.
- The school ICT systems may not be used for private purposes, unless the Headteacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised – do not load unauthorised software. Authorisation to be obtained from the Network Manager only.
- You must not attempt to access restricted areas or blocked sites.
- If inappropriate material is displayed on your computer you must notify your teacher or in the case of staff your line-manager.
- Irresponsible use may result in the loss of Internet access.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Signed_________________________________

Name (Printed)____________________________