SHIRLEY HIGH SCHOOL
PERFORMING ARTS COLLEGE

E- Safety Policy (including Staff Acceptable Use Policy and Student Guidelines for Network and Internet Use and Responsible Internet Use Policy)

Mission statement: We deliver high quality teaching and learning in an environment that meets the needs of our students, so that all achieve and enjoy.

Philosophy

Shirley High School Performing Arts College promotes a safe learning environment where everyone feels able to enjoy and achieve and where success is recognised and rewarded. We recognise that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents/carers use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for all who work with children; and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our Anti Bullying Policy.

Principles

The school will ensure that:

- E-Safety guidance is given to students on a regular and meaningful basis.
- E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.
- The school has a framework for teaching internet skills in ICT lessons.
- The school provides opportunities within a range of curriculum areas to teach about E-Safety.
- Educating students about the online risks e.g. sexual exploitation, radicalisation, identity fraud etc., that they may encounter outside school is done informally when opportunities arise and as part of the PSHEE curriculum.
- Students are taught about copyright, respecting other people's information, safe use of images and learn good teaching skills through ICT and other curriculum areas.
- Students are aware of the impact of cyber-bullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP (Child Exploitation and Online Protection Centre) report abuse button.
- All staff sign the school's Acceptable Use Policy and all new staff receive information on the school's Acceptable Use Policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

- All students and parents / carers sign the Student Guidelines for Network and Internet Use Policy in the student planners at the start of each school year.
- E-Safety posters are prominently displayed in all ICT suites.

Roles and Responsibilities

The Principal is ultimately responsible for the E-Safety of all students and staff. All staff, students, parents and governors should be made aware of the policy along side awareness being raised of the issues associated with E-Safety in schools.

The School IT Network Manager has the following responsibilities:

- Reviewing and managing the security of the computers, school information systems and internet networks as a whole.
- Protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats.
- Regularly reviewing and updating virus protection software.
- Ensuring that unapproved software is not downloaded to any school computers.
- Enforcing the use of user logins and passwords to access the school network.

The Head of ICT & Business has the following responsibilities:

- Monitoring of the Student Guidelines for Network and Internet Use Policy. (Appendix 2)
- Applying sanctions as appropriate for students who violate the rules included in this policy.

School staff have the following responsibilities:

- Sign and adhere to the Acceptable Use Policy (Appendix 1)
- Report any breaches of the policy

Students have the following responsibility:

- Sign and adhere to the Student Guidelines for Network and Internet Use policy printed in the student planners.
- Post-16 students to sign and adhere to the ‘Bring Your Own Device Agreement’. (Appendix 4)

Parents have the following responsibilities:

- To be fully involved with promoting E-Safety both in and outside of school.
- To monitor internet and mobile data usage and use parental controls as appropriate for the age of the child.
- To read through and sign a User Agreement and Parental Permission form on behalf of their child on admission to the school. (Appendix 2)
- To read through and sign a SIMS Learning gateway (SLG) User Agreement and Parental permission form on behalf of their child. (Appendix 3)
- To read through and sign a Bring Your Own Device Agreement for Sixth Formers, if applicable. (Appendix 4)
- To sign the Responsible Internet Use Policy form in the Student Planner annually.
- To make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website) through ticking the appropriate box on the Contact Details Form completed on their child’s admission to school.
- To sign the Media Consent Form in the Student Planner annually as applicable.

There are some helpful resources for parents/carers below, which we encourage you to read in order to help your child stay safe online.

http://www.internetmatters.org/
https://ceop.police.uk/

Making use of ICT and the internet in school

The internet is used in school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school’s management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies.

Policy and guidance of safe use of children's photographs and work

Colour photographs and students' work bring our school to life, showcase our students' talents, and add interest to publications both online and in print that represents the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website) through ticking the appropriate box on the Contact Details Form. They will then sign the Media Consent Form in the Student Planner annually as applicable. The school does this so as to prevent repeatedly asking parents/carers for consent over the school year, which is time-consuming for both parents/carers and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students.

Use of cameras / video recorders by staff

Staff are expected to use school equipment to take photos or record videos of students. Staff are not permitted to use personal digital cameras, camera phones or video recording devices in school or on a school related activity or store images at home, without permission from a senior manager.

Images / recording of students recorded on school equipment should be stored sensitively and deleted as soon as they are no longer required. If images / recordings of students need to be stored for a longer period of time they should be stored on a school computer in a clearly labelled file. On no account should images / recordings of students be transferred onto or stored on personal equipment without permission from a senior manager. Ex members of staff will be expected to ensure they do not have images or recordings of students from the school once they have left, without permission from a senior manager and the parents / carers.

Mobile phones and personal devices

While mobile phones and electronic devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material

- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school therefore does not allow students in Years 7 - 11 to be in the possession of mobile phones or other electronic devices in school. If seen they will be confiscated. This rule is not enforced for students on school trips.

Staff are not permitted to use their mobile phones during a lesson, have them visible to students during a lesson or use their mobile phones in front of students around the school. The use of a mobile phone is restricted to the staffroom, office or classroom when students are not present, when in school.

The school will not tolerate cyber-bullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined.

Protecting personal data

The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the police. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Links with other policies

This policy has been developed and evaluated with a view to regulating ICT activity in school, and providing a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours.

It links with the following policies which can be read in conjunction:

- Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Teaching and Learning Policy
- Data Protection Policy
- CCTV Policy
- Staff Code of Conduct

Evaluation and Monitoring

This policy is a dynamic document and will be updated as new guidance is produced or, in response to research, review or other events that have not previously been covered in depth.

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Appendix 1

SHIRLEY HIGH SCHOOL
STAFF ACCEPTABLE USE PROCEDURE COMPUTERS
(for all Staff - Teaching and Support)

This memorandum is for all staff. It contains important procedures related to confidentiality and sensitive issues. Please remember that staff are responsible for the safe keeping and correct use of all the technical equipment in the classrooms that they use.

1. Staff must lock or log off computers at all times when away from their rooms/offices.
2. The contents of SIMS, the staffroom in Fronter (MLE), Outlook e-mail nor calendar, or any other sensitive information must not be visible on a classroom display device of any kind, or if the screen may be seen by a student or outside party.
3. Do not disclose your network password to anyone, including other staff. Do not disclose your MLE (Fronter) password to anyone – this also gives them access to your emails.
4. Do not enter the file areas of other staff without their permission first.
5. Do not publish the names or images of students without the permission of parents first.
6. You must comply with Data Protection by ensuring that any data you keep about students is kept private
7. Abide by copyright. This applies to text, graphics, images, audio and videos. Generally if you want to reproduce it – ask permission first.
8. This Acceptable Use Policy applies to both your use of computer systems inside and outside school.
9. If using Remote Access, it is essential that any accessed programs are closed correctly and completely, and that no unauthorised person will have access.

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the School Business Manager.

I agree to report any misuse of the network to the School Business Manager.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to the School Business Manager.

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the School Business Manager.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

This acceptable use policy should be read in conjunction with the Child Protection policy.

Staff Name: ____

Staff Signature: _______________________________

Date: _ _ /_ _ /_ _ _ _

PLEASE RETURN SIGNED COPY OF THIS FORM TO THE GENERAL OFFICE.

Appendix 2

Dear Parent(s)/Carer(s)

Internet and E-Mail Access for Students

As part of the school's ICT programme we offer students supervised access to the Internet. Before the school allows students to use the Internet and e-mail, we require all students to obtain parental permission and both they and you must sign and return the attached form as evidence of your approval and their acceptance of the school rules on this matter.

Students are issued with a unique username and password when they enter the school. The code gives the student access to the computer system, it is their personal code and should not be disclosed to anyone else.

During school, teachers will guide students towards appropriate materials on the Internet. Although the school provides filtered and secure Internet access, parents and guardians should be warned that some students may find ways to access material which is inaccurate, defamatory, illegal or potentially offensive to some people. Students who misuse or abuse Internet or e-mail access at school will face disciplinary action and may lose their right to Internet access for a fixed term.

So far the school has operated simple common sense rules, and students have understood the consequences of them attempting to access unsuitable a material or to use the facilities inappropriately. In short, they have had their access rights taken away from them. In the case of future contravention of these common sense rules the school reserves the right to suspend or withdraw completely the access that any student has to the network, Internet (including Fronter) or to email facilities.

Please read through the attached documents carefully and then complete the attached **Internet and Electronic Mail User Agreement and Parental Permission Form** with your son/daughter and return it to school with all other forms.

Yours sincerely

CRixson

Mrs C Rixson
Head of ICT & Business

Student Guidelines for Internet & Network Use

General

- Students are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. General school rules apply.
- The Internet is provided for students to conduct research and communicate with others. **Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility.**
- **Individual users** of the Internet **are responsible for their behaviour** and communications over the network. It is presumed that users will comply with school standards and will honour the agreements they have signed.
- Students **should not** give out personal information (including photos) of themselves or others when on the Internet or in e-mails.
- Computer storage areas, usb pen drives etc will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or other media will always be private.
- All students have the responsibility for the security of their username and password. They **must not** allow other students to access the network/internet using their log-on details. Students must report any evidence or suspicion that anyone knows their password to Mrs Rixson (Head of ICT & Business).
- Students are personally responsible for any actions/ activities carried out on the network under their username.

The following are not permitted:

1. **SENDING OR DISPLAYING OFFENSIVE MESSAGES OR PICTURES**
2. **USING THE NETWORK OR INTERNET TO SEND OFFENSIVE OR HARASSING MATERIALS TO OTHERS**
3. **DAMAGING COMPUTERS AND COMPUTER PERIPHERALS (PRINTERS, SCANNERS, CAMERAS ETC)**
4. **ACCESSING UNDESIRABLE MATERIAL SUCH AS OBSCENE, HATEFUL OR PORNOGRAPHIC MATERIAL ETC**
5. **DOWNLOADING AND/OR RUNNING PROGRAMS THAT HAVE NOT BEEN INSTALLED BY THE SCHOOL IT TECHNICIANS**
6. **VIOLATING COPYRIGHT LAWS (PASSING OFF CONTENT FOUND ON THE INTERNET AS YOUR OWN)**
7. **TO LOG ON USING ANOTHER STUDENTS' USER ID/PASSWORD**
8. **TO USE ANOTHER STUDENTS' ACCESS TO THE INTERNET**
9. **TO ALLOW ANOTHER STUDENT TO USE YOUR USERNAME AND PASSWORD**
10. **EXCHANGING PASSWORDS**
11. **TRESPASSING IN OTHERS' FOLDERS, WORK OR FILES**
12. **PRINTING DOCUMENTS UNNECESSARILY**
13. **UNAUTHORISED USE OF THE INTERNET DURING LESSON TIME.**
14. **DOWNLOADING OF FILES (FROM INTERNET OR A USB PEN DRIVE ETC) THAT ARE NOT RELEVANT TO THE CURRICULUM**
15. **USING THE SCHOOL COMPUTER RESOURCES TO PRINT AND/OR PUBLISH ANYTHING THAT IS NOT DIRECTLY RELATED TO SCHOOL WORK.**
16. **PLAYING GAMES OR GAMBLING ON THE INTERNET, INTERNET SHOPPING, VISITING SOCIAL NETWORKING SITES OR SMS MESSAGING VIA WEBSITES.**
17. **BYPASSING (OR ATTEMPTING TO BYPASS) THE SCHOOL INTERNET FILTERING SYSTEM TO ACCESS WEBSITES**

Sanctions

1. Violations of the above rules will result in a temporary ban (of 1 half-term or equivalent) or a permanent ban on Internet use, which may also include network use.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.

SHIRLEY HIGH SCHOOL PERFORMING ARTS COLLEGE

Internet and Electronic Mail

User Agreement and Parental Permission Form

Student

I have read and understand the information outlined on the "**Student Guidelines for Internet & Network Use"** document.

I agree to comply with the school rules on its use. I will use the school network and Fronter in a responsible way and observe **all** the restrictions laid down by the school.

I understand that if I break any of the rules listed in the "**Student Guidelines for Internet & Network Use**" document I will be temporarily or permanently denied Internet access at school and/or access to the school network.

Student Name ___________________________________ **Year Group/Form** __________

Student Signature __________________________________ **Date: ___/___/___**

Parent/Carer

I have read and understand the information outlined on the "**Student Guidelines for Internet & Network Use"** document.

As the parent / carer of the student above, I grant permission for my son or daughter to use e-mail and the Internet. I understand that my son or daughter will be held accountable for their own actions and will face disciplinary action if they misuse or abuse the Internet or e-mail. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media.

Parent/Carer Signature ____________________________

Date: ___/___/___

Appendix 3

SHIRLEY HIGH SCHOOL PERFORMING ARTS COLLEGE
SLG ACCEPTABLE USE POLICY REPLY SLIP

TO: **Mrs K Walpole – Principal's PA / Head of Admin**
RE: **Student Name(s) – SLG: Acceptable Use Policy and Password Request**

LEARNING GATEWAY GUIDELINES

- Do not let anyone else (including the relevant student) have access to your username and password
- Do not set your browser to remember your username and password
- Remember to log out of SIMs Learning Gateway and close your internet browser each time you finish a session

Parental Responsibility Contact 1
Name:
Relationship to child/children:
I confirm that I have Parental Responsibility for the above mentioned child/children. □
Please send me a password to access SIMs Learning Gateway Email address:……………………………………………………………………………………….. (Block Capitals Please)
I do not wish to sign up to SIMs Learning Gateway and would like to receive paper copies of progress reviews whilst my child/children attend Shirley High School. I understand that this will not change unless I inform the school accordingly. □
I have read the SIMs Learning Gateway Parents/Carers' Acceptable Use Policy, including the user guidelines and I agree to abide by and support these rules. I understand that if I violate any terms of this Acceptable Use Policy that I may lose my privileges to use the Learning Gateway.
Signature………………………………………………….. Dated…………………………………

Parental Responsibility Contact 2 (only if applicable)
Name:
Relationship to child/children:
I confirm that I have Parental Responsibility for the above mentioned child/children. □
Please send me a password to access SIMs Learning Gateway Email address:……………………………………………………………………………………….. (Block Capitals Please)
I do not wish to sign up to SIMs Learning Gateway and would like to receive paper copies of progress reviews whilst my child/children attend Shirley High School. I understand that this will not change unless I inform the school accordingly. □
I have read the SIMs Learning Gateway Parents/Carers' Acceptable Use Policy, including the user guidelines and I agree to abide by and support these rules. I understand that if I violate any terms of this Acceptable Use Policy that I may lose my privileges to use the Learning Gateway.
Signature………………………………………………….. Dated…………………………………

SIMs LEARNING GATEWAY
PARENTS'/CARERS' ACCEPTABLE USE POLICY

Your account will become active once the school receives your signed copy of the Acceptable Use Policy / User Guidelines, as outlined below.

PLEASE KEEP A COPY FOR YOUR RECORDS

1. Parents/Carers will have access to the following data about their child:
   - Attendance
   - Achievement Points and Commendations
   - Progress
   - Homework Set
   - Behaviour
   - Timetable
   - Written Reports and Termly Reports
2. A username and password are required to access SIMs Learning Gateway. These details must not be shared with anyone (including students). Parents should not set their Learning Gateway password.
3. A password will be provided when the school has received a signed copy of the Acceptable Use Policy by post.
4. Parents/Carers should ensure their email address is correct and define a security question at the first login to SIMs Learning Gateway.
5. Parents/Carers may change their password at any time after logging in to SIMs Learning Gateway.
6. Parents/Carers must not attempt to alter or destroy data relating to their own children, another user or the school.
7. Parents/Carers must not use SIMs Learning Gateway for any illegal activity, including violation of the Data Protection Act.
8. Parents must not access data or any account that is not assigned to them.
9. Shirley High School reserves the right to revoke an individual's access at any time for inappropriate use of SIMs Learning Gateway. Inappropriate use includes, but is not limited to, the use of inappropriate or offensive language, the introduction of material which is considered unsuitable or attempting to deliberately introduce computer viruses onto the school system.
10. Violation of the terms of this Acceptable Use Policy will lead to access being withdrawn. In the case of a serious violation that infringes the law, the police will be informed.

PLEASE REVIEW THE QUICK START USER GUIDELINES ATTACHED BEFORE SIGNING THIS DOCUMENT

Appendix 4

Re: BRING YOUR OWN DEVICE AGREEMENT FOR SIXTH FORMERS

In order to maximise opportunities for and approaches to learning, and recognising the importance of our expanding Virtual Learning Environment, we are introducing a new procedure whereby sixth form students can bring in their own laptops, or other appropriate electronic devices, and use them for private study and research in the sixth form study centre.

To make this work, we need your daughter / son to have to have read the ‘Student Guidelines for Internet & Network Use’ which is attached to this letter. This information can also be found on the school website under ‘Parents Info - Forms’. We would also like you to indicate that you have discussed this with your son / daughter to ensure that this is fully understood. **We ask you and your son / daughter to keep this document in an accessible place and to sign and return the declaration slip below if you wish to take up this opportunity.**

Sixth form students who sign this letter and indicate that they have understood and will abide by the relevant guidelines will then have monitoring software put on their devices by an IT Technician(this software only works when students use their SHS user ID and the school network, not when offsite). Once this has been completed they will be provided with an identification number for their device and will be able to connect to the school’s Wi-Fi, as well as to use their SHS user ID and password to access the network.

Yours sincerely

B.S. Doherty

Ms B Doherty
Vice Principal – Head of Post 16

BYOD Agreement for Sixth Formers - Reply Slip to Mrs Kelly

I hereby certify that I will (tick as appropriate)

□ Be responsible for the security, maintenance and insurance of my own device. The school takes no responsibility for damage or loss
□ Ensure that I have the best practice anti-virus software
□ Ensure that I use my device for learning and school work
□ Abide by the ‘Student Guidelines for Internet and Network Use’
□ Keep secure my personal addresses, telephone numbers and those of others
□ Not access or download materials which could make others feel uncomfortable
□ Not visit chatrooms and/or other social media sites
□ Be aware of the sanctions which may result from the misuse of electronic devices
□ Agree to allow the school to install monitoring software on my device

Student Name…………………………………………………….. Tutor Group …..…

Signed Student ………………………………………………… Date ………….

Signed Parent/Carer………………………………………………… Date ……....

Appendix 5
SOCIAL MEDIA

1. INTRODUCTION

This guidance applies to Shirley High School students, staff, parents and the wider school community. It covers personal use of social media, as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.

This guidance applies to personal web space such as social networking sites (for example Facebook, Instagram, Snapchat), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as Flickr and YouTube.

Since it is impossible to cover all circumstances or emerging media, the principles set out in this guidance should be followed irrespective of the medium.

2. GUIDELINES FOR STUDENTS

2.1. Your online behaviour should reflect the same standards of honesty, respect and consideration that you use face-to-face.

2.2. Your use of social media should be age appropriate e.g. only over 13s should be using Facebook.

2.3. When posting comments or photos on social media channels, ask yourself whether you would be happy for your parents or your future employer to read your posts.

2.4. Provide as little information about yourself as possible; not providing your date of birth or location will improve your online security.

2.5. You should set your privacy settings on Facebook to ‘Friends Only’, but be aware that unless your friends’ settings are the same as yours, your posts may be seen more widely.

2.6. Think carefully before engaging with strangers in ‘open’ environments, especially Twitter; be aware that protecting your tweets will improve your online security

2.7. Do not attempt to ‘friend’ or ‘follow’ staff on social media sites

2.8. Do not tag or identify yourself (or other students) on Shirley High social media sites; even when using your own accounts, you should ask permission before tagging someone in a photo.

2.9. Do not engage in any activities involving social media which might bring Shirley High into disrepute

2.10. Do not engage in any abusive, threatening, unkind or bullying behaviour.

2.11. Use of profanity or threatening language is not acceptable

2.12. Under no circumstances should negative comments be made about staff, parents or other students on social media sites

2.13. Shirley High reserves the right to monitor social media activity and if students are found contravening the guidelines, the school sanctions will be imposed.

3. GUIDELINES FOR PARENTS

3.1. The school will monitor, and where appropriate, moderate, content and activity on Shirley High social media platforms

3.2. The school cannot be held responsible for improper use of social media by students

3.3. We ask that any comments posted on school social media accounts are constructive and not seen as vehicle for questions that require immediate response. Negative comments or complaints should be made using correct procedure.

4. USING SOCIAL MEDIA FOR MARKETING SHIRLEY HIGH SCHOOL

The Administration team runs the school’s official website and social networking for marketing. If you have any concerns about content you have viewed on school social media sites, you should contact office@shirley.croydon.sch.uk.

While students and the wider school community are encouraged to interact with these social media sites they should do so with responsibility and respect.

If staff wish to set up dedicated social media accounts for their subjects, they should first discuss this with the Principal and Principal’s PA.

5. BREACHES OF THIS APPENDIX

Any breach of this guidance that leads to a breach of confidentiality, defamation or damage to the reputation of Shirley High School or any illegal acts or acts that render Shirley High liable to third parties may result in legal action, disciplinary action or sanctions in line with the published school policies for staff and students.