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

INTENT

Shirley High School promotes a safe learning environment where everyone feels able to enjoy and achieve and understands that electronic communication is a growing part of life outside of school. We have a responsibility to safeguard our school community against potential dangers when accessing the internet at school, and to educate our school community about how to protect themselves online when outside of school. E-safety and the appropriate use of social media is a whole-school issue and responsibility. This policy therefore applies to Shirley High School students, staff, parents and the wider school community.

Keeping Children Safe in Education 2025 (KCSIE 2025) identifies four areas of online risk: Content, Conduct, Conduct and Commerce. E-safety refers to the safe use of a range of technological devices and platforms including the internet, mobile phones and other electronic communities devices and technologies that can be used to expose children to risk or harm under these categories. We know that some adults, children 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. Educating all members of the school community on the risks and responsibilities of e-safety falls under the duty of care of those working with children.

Cyber-bullying will be managed through our anti-bullying procedures which are outlined in our Anti Bullying Policy. However, the school does place the onus on parents to monitor and control their child's use of the internet, social media and other online technologies and devices. As such, the school will use their discretion when intervening in issues related to E-Safety outside of school and we may refer families to relevant authorities and agencies if we believe that parents are not displaying appropriate care and attention to their child's safety and wellbeing while using aforementioned technology and devices.

This policy aims to be an aid in regulating the use of technology, internet and devices in school, and provide a good understanding of appropriate use of technology, internet and devices that members of the school community can use as a reference for their conduct online outside of school hours.

Anyone found in serious breach of this policy will be sanctioned accordingly which may include (not limited to) a temporary or indefinite ban prohibiting them from using the school's IT systems.

IMPLEMENTATION

The school will:

- Educate students about online risks e.g. sexual exploitation, radicalisation, identity fraud etc., that they may encounter outside school through their digital literacy and PD lessons. This will include an awareness of the KCSIE 2025 updates regarding misinformation and conspiracy theories.
- 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.
- Provide Online Safety Training for staff.
- Ensure all staff are aware of and have agreed to the Acceptable Use Policy.
- Make all staff 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.
- Include Acceptable Use information and policy in our student admission and induction process.

Roles and Responsibilities

The Principal is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents and students are aware of their responsibilities in relation to social media use.
- Promoting safer working practices and standards with regards to the use of social media for all staff, students, parents and governors.
- Establishing clear expectations of behaviour for social media use.
- Ensuring that this policy, as written, does not discriminate on any grounds, including, but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- In conjunction with the governing board, handling complaints regarding this policy and its provisions in line with the school's Complaints Procedures Policy.
- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.
- Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.
- Working alongside the IT network manager, data protection officer (DPO) and Designated Safeguarding Lead (DSL) to ensure appropriate security measures are implemented and compliance with the GDPR.

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.
- Monitoring of the Student Guidelines for Network and Internet Use Policy. (Appendix 2)

The Deputy Principal - Pastoral / DSL has the following responsibilities:

- Annual review of the E Safety & Social Media Policy
- Provision of annual staff Online Safety training
- Applying sanctions as appropriate for students who violate the rules included in this policy
- Monitor and delegate a team of staff to monitor the internet use of students through the school's monitoring system (i.e Smoothwall)

School staff have the following responsibilities:

- Sign and adhere to the Acceptable Use Policy (Appendix 1)
- Report any breaches of the policy
- Undertake Online Safety training
- Read and adhere to the guidelines in the Remote Learning Policy
- Ensure students adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.
- Reporting any social media or IT misuse by staff, students or parents to the DSL, DPO or Principal immediately.

Students have the following responsibility:

- Sign and adhere to the Student Guidelines for Network and Internet Use policy signed on admission to the school
- Post-16 students to sign and adhere to the 'Bring Your Own Device Agreement'. (Appendix 4)
- Be aware of and adhere to the guidelines relating to them in the Remote Learning Policy
- Ensure they understand how to use social media appropriately and stay safe online.

Parents/Carers have the following responsibilities:

- To be fully involved with promoting E-Safety and Online Safeguarding 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 take appropriate responsibility for their use of social media and the influence on their children at home.
- 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 the Parents/Carers' Acceptable Use Policy. (Appendix 3)
- To read through and sign a Bring Your Own Device Agreement for Sixth Formers, if applicable. (Appendix 4)
- 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 Consent Form completed on their child's admission to school.
- To read online safeguarding information disseminated by the school and attend information meetings on this subject where organised by the school wherever possible.
- To ensure that their children are accessing age appropriate internet and social media platforms.
- Accountability for their child's use of internet, social media and technology outside of school.

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/

https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Educated for a Connected World

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

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 Consent Form. 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 of 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 must 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.

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. Staff leavers are 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.

As a preventative measure, the school 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. Please refer to the school's behaviour policy regarding mobile phones in school. This rule is not enforced for students on school trips.

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 sanctioned.

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 how the 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.

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

This policy has due regard to legislation and guidance including, but not limited to, the following:

- The General Data Protection Regulation (GDPR)
- DfE (2018) 'Data protection: a tool kit for schools'
- The Data Protection Act 2018

SOCIAL MEDIA POLICY

INTENT

This guidance 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.

For the purpose of this policy, the school defines "social media" as any online platform that offers real-time interaction between the user and other individuals or groups including, but not limited to, the following:

- Blogs, podcasts
- Online discussion forums, such as netmums.com
- Collaborative spaces, such as Facebook
- Media-sharing devices, such as YouTube
- 'Micro-blogging' applications, such as X (formerly known as Twitter)
- Chatrooms
- Open access online encyclopaedias such as Wikipedia
- Social bookmarking sites such as del.icio.us.

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.

We are committed to:

- Encouraging the responsible use of social media by all staff, parents and students in support of the school's mission, values and objectives.
- Protecting our students from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.
- Ensuring parents / carers are provided with E-Safety information.

IMPLEMENTATION

Data Protection Principles

- The school will obtain consent from students and parents on entry to the school on the school information form, which will confirm whether or not consent is given for posting images and videos of a student on social media platforms. The consent will be valid for the students' time at Shirley High School.
- A record of consent is maintained, which details the students for whom consent has been provided. The Principal's PA / DPO is responsible for ensuring this consent record remains up-to-date.

- Where a student is assessed by the school to have the competence to understand what they are consenting to, the school will obtain consent directly from that student; otherwise, consent is obtained from whoever holds parental responsibility for the child.
- Parents and students are able to withdraw or amend their consent at any time. To do so, parents and students must inform the school in writing.
- Consent can be provided for certain principles only, for example only images of a student are permitted to be posted, and not videos. This will be made explicitly clear on the consent form provided.
- Where parents or students withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents' and students' requirements following this.
- Wherever it is reasonably practicable to do so, the school will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.
- The school will only post images and videos of students from whom consent has been received.
- Only school-owned devices or devices that have been pre approved by a member of SLT will be used to take images and videos of the school community
- When posting images and videos of students, the school will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a student being identified.
- The school will not post students' personal details on social media platforms.
- Students' full names will never be used alongside any videos or images in which they are present.
- Only appropriate images and videos of students will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a student in swimwear.
- When posting on social media, the school will use group or class images or videos with general labels, e.g. 'sports day'.
- Before posting on social media, staff will refer to the consent record log to ensure consent has been received for that student and for the exact processing activities required; ensure that there is no additional identifying information relating to a student.
- Any breaches of the data protection principles will be handled in accordance with the school's GDPR Policy and the necessary procedures will be followed by the DPO.
- Consent provided for the use of images and videos only applies to school accounts – staff, students and parents are not permitted to post any imagery or videos on personal accounts.

GUIDELINES FOR STAFF

School accounts

- School social media passwords are kept in the Principal's PA's office – these are not shared with any unauthorised persons, including students, unless otherwise permitted by the Principal.
- Staff will ensure any posts are positive in nature and relevant to students, the work of staff, the school or any achievements.
- If staff wish for reminders to be posted for parents, e.g. returning slips for a school trip, staff will seek permission from the Principal before anything is posted.
- Staff will adhere to the data protection principles outlined in this and the GDPR policy at all times.
- Staff will not post any content online which is damaging to the school or any of its staff or students.
- If inappropriate content is accessed online, a report form will be completed and passed on to the DSL. The DPO retains the right to monitor staff members' internet usage in line with the GDPR Policy.

Personal accounts

- Staff members will not access social media platforms during lesson times.
- Staff members will not use any school-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the Principal.
- Staff members are permitted to use social media during break times.

- Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the Principal, and once the IT Network Manager has ensured the necessary network security controls are applied.
- Staff will avoid using social media in front of students.
- Staff will not "friend" or otherwise contact students or parents through their personal social media accounts.
- If students or parents attempt to "friend" a staff member they will report this to the DSL.
- Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to students or parents – any contact with students or parents will be done through authorised school contact channels.
- Staff members will ensure the necessary privacy controls are applied to personal accounts.
- No staff member will post any content online that is damaging to the school or any of its staff or students.
- Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not that of Shirley High School.
- Staff members will not post any information which could identify a student, class or the school – this includes any images, videos and personal information.
- Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.
- Staff members will not post anonymously or under an alias to evade the guidance given in this policy.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
- Members of staff will regularly check their online presence for negative content via search engines.
- Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.
- Members of staff will not leave a computer or other device logged in and unlocked when away from their desk.
- Staff members will use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.
- Any personal or familial relationships with students or their families will be declared to the DSL and the Principal to explain any conflict of interest that this policy may create for a member of staff.

GUIDELINES FOR STUDENTS

- Your online behaviour should reflect the same standards of honesty, respect and consideration that you use face-to-face.
- Your use of social media should be age appropriate e.g. only over 13s should be using Facebook.
- 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.
- Provide as little information about yourself as possible; not providing your date of birth or location will improve your online security.
- 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.
- Think carefully before engaging with strangers in 'open' environments, especially Twitter; be aware that protecting your tweets will improve your online security
- Do not attempt to 'friend' or 'follow' staff on social media sites
- 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.
- Do not engage in any activities involving social media which might bring Shirley High into disrepute
- Do not engage in any abusive, threatening, unkind or bullying behaviour.

- Use of profanity or threatening language is not acceptable
- Under no circumstances should negative comments be made about staff, parents or other students on social media sites
- Shirley High reserves the right to monitor social media activity and if students are found contravening the guidelines, the school sanctions will be imposed and external agencies may be involved.
- Students will not post anonymously or under an alias to evade the guidance given in this policy.

GUIDELINES FOR PARENTS/CARERS

- The school will monitor, and where appropriate, moderate, content and activity on Shirley High social media platforms
- The school cannot be held responsible for improper use of social media by students
- Parents/Carers will not attempt to "friend" or otherwise contact members of staff through their personal social media accounts. Parents/Carers are only permitted to be affiliates of school social media accounts.
- Parents/Carers will not post anonymously or under an alias to evade the guidance given in this policy.
- Parents/Carers will not post any content online which is damaging to the school or any of its staff or students.
- 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 the correct procedure.
- Confirm any personal or familial relationship with members of staff to explain any conflict of interest that this policy may cause.

CYBER-BULLYING

- Cyber bullying incidents are taken seriously at Shirley High School. Any reports of cyber bullying on social media platforms by students will be handled in accordance with the Anti-Bullying (inc. Cyber-Bullying) Policy.
- Allegations of cyber bullying from staff members will be handled in accordance with the Allegations of Abuse Against Staff in the Child Protection Policy.
- Staff members will not respond or retaliate to cyber bullying incidents. Incidents will be reported as inappropriate, and support will be sought from the DSL.
- Evidence from the incident will be saved, including screen prints of messages or web pages, and the time and date of the incident.
- Where the perpetrator is a current student or colleague, most incidents can be handled through the school's own disciplinary procedures.
- Where the perpetrator is an adult, in nearly all cases, a member of the SLT will invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.
- If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school will consider whether the police should be contacted.
- As part of the school's ongoing commitment to the prevention of cyber bullying, online safeguarding information, online safeguarding education and discussion about e-safety will be disseminated to parents / carers and form part of the content of the school's PD programme.

BLOCKED CONTENT

- The school has installed firewalls on the school's network to prevent access to certain websites.
- Attempts made to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.
- Inappropriate content accessed on the school's computers will be reported to IT Network Manager on the inappropriate content accessed form (Appendix 5) so that the site can be blocked.
- The DPO retains the right to monitor staff and student access to websites when using the school's network and on school-owned devices.
- Requests may be made to access erroneously blocked content by submitting a blocked content access form (Appendix 5) to the IT Network Manager.

USING SOCIAL MEDIA FOR MARKETING SHIRLEY HIGH SCHOOL

SLT 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.

TRAINING

- At Shirley High School, we recognise that early intervention can protect students who may be at risk of cyber bullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk students when they undergo their annual safeguarding training.
- Teachers and support staff will also receive this training as part of their new starter induction.
- Students will be educated about e-safety and appropriate social media use through a variety of mediums, including: assemblies, PD lessons and cross-curricular links.
- Training for all students, staff and parents/carers will be refreshed in light of any significant incidents or changes.

BREACHES OF THIS GUIDANCE

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.

IMPACT

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.

All members of the school community are to be aware of the dangers of using the internet and how they should conduct themselves online.

Links

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

- Child Protection Policy
- Staff Code of Conduct
- Behaviour Policy
- Anti-Bullying Policy (inc Cyber Bullying)
- Teaching and Learning Policy

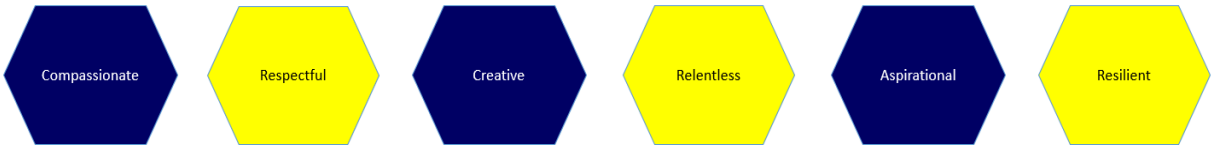
- Data Protection Policy
- CCTV Policy
- Use of EBay policy
- Remote Learning Policy
- Data and E-Security Breach Prevention and Management Plan

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.

We want all at SHS to believe in and maintain the values of our school:



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, Google Drive and associated features, G-mail or 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 Google Drive password to anyone.
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/carers 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 Code of Conduct, and the Data and E-Security Breach Prevention and Management Plan

Staff Name: _____

Staff Signature: _____

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

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

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 carers 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.

Shirley High School operates simple common sense rules, and students understand the consequences of them attempting to access unsuitable material or to use the facilities inappropriately. This includes access rights taken away, accounts suspended and in certain cases completely withdrawn. In the case of future contravention of these common sense rules the school reserves the right to suspend or withdraw completely.

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

Shirley High School 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 **must not** give out personal information (including photos) of themselves or others when on the Internet or in e-mails.
- Computer storage areas 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 their Head of Year.
- 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 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
18. The recording - video and / or audio of any member of the Shirley High staff at any time is not permitted unless permission has been given by the member of staff.

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

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network 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.

Student Name _____ Year Group/Form _____

Student Signature _____ Date: ___/___/___

Parent

As the parent or legal guardian of the student signing above, I grant permission for my son or daughter to use Electronic Mail and the Internet. I understand that students will be held accountable for their own actions and will face disciplinary action if they misuse or abuse the Internet or Electronic 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

ELECTRONIC HOME / SCHOOL COMMUNICATION

PARENTS'/CARERS' ACCEPTABLE USE POLICY

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

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 unique registration email is required to access the Class Charts App. These details must not be shared with anyone (including students).

3. Parents/Carers must not attempt to alter or destroy data relating to their own children, another user or the school.

4. Parents/Carers must not use Class Charts App for any illegal activity, including violation of the Data Protection Act.

5. Parents must not access data or any account that is not assigned to them.

6. Parents must not record - video or audio members of the school community. Permission must be requested to record any meetings with Shirley High staff.

7. Shirley High School reserves the right to revoke an individual's access at any time for inappropriate use of Class Charts App. 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.

8. 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.

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

Mr M Cotton

Assistant Principal – 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

Blocked content access request form

Requester	
Staff name:	
Date:	
Full URL:	
Site content:	
Reasons for access:	
Identified risks and control measures:	
Authoriser	
Approved?	**✔ / X**
Reasons:	
Staff name:	
Date:	
Signature:	

Inappropriate content report form

Staff name (submitting report):	
Name of individual accessing inappropriate content (if known):	
Date:	
Full URL(s):	
Nature of inappropriate content:	
To be completed by e-safety officer	
Action taken:	
Staff name:	
Date:	
Signature:	