PATCHAM HIGH SCHOOL

One Team, One Dream

# Acceptable use of ICT and E-Safety

**PATCHAM HIGH SCHOOL**

**SCHOOL POLICY ON ACCEPTABLE USE OF ICT AND E-SAFETY**

**INCLUDING SOCIAL NETWORKING POLICY**

**Status: Additional**

**Purpose**

This document sets out our policy on maintaining safe and secure practice pertaining to the use of ICT hardware, software and electronic communication. (For the purposes of this policy electronic communication includes: social networking sites, blogs, the World Wide Web, mobile phones, e-mail, web cams, video conferencing and wireless games consoles.)

**Rationale**

The use of new and emerging technologies is a vital part of the work of schools. Internet use is part of the statutory curriculum and a necessary tool for learning. At Patcham High school staff and students have access to a wide range of industry standard and educational software to enhance learning. The Internet and the World Wide Web is a powerful learning tool to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.

The increasing use of technology in all aspects of society makes confident, creative and productive use of ICT an essential skill for life. ICT capability encompasses not only the mastery of technical skills and techniques, but also the understanding to apply these skills purposefully, safely and responsibly in learning, everyday life and employment. ICT capability is fundamental to participation and engagement in modern society. Students use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security both in and out of school. All steps will be taken by the school to ensure the safety and security of staff and students whilst using ICT technology.

**Relationship to other policies**

This policy relates to those on Health & Safety, Child Protection, Whistle Blowing, Safer Recruitment, Anti-bullying and Behaviour.

**Key Principles**

At Patcham High school our common purpose is to ensure that both staff and students use ICT software, hardware and electronic communication to enhance learning and teaching. We will ensure that risk is minimised and that all stakeholders are well informed about safe and acceptable use of ICT and electronic communication.

**Roles and Responsibilities**

| Governing Body | The Head Teacher | All Staff | e-Safety Co-Ordinator |
|---|---|---|---|
| •Ensure, as far as is reasonably practicable, the health, safety and welfare of all staff and students whilst in school | •Ensure that every member staff is aware of the contents of this policy<br>•Monitor compliance by staff with the policy<br>•Seek remedies in law where appropriate<br>•Delegate action to the appropriate person (s) where appropriate<br>•Appoint an e-Safety Coordinator. | •Maintain awareness and compliance with the policy<br>•By default, consent to the monitoring and surveillance of e-mail, Internet and workstations.<br>•Support and promote e-safe behaviours in the classroom.<br>•Report incidents to their line manager<br>•Read and sign the ICT Acceptable use Agreement<br>•Register social networking accounts with the e-Safety Co-Ordinator | •Monitor incidents and keep records<br>•Liaise with the Head teacher and other members of staff including the child protection officer over incidents<br>•Inform parents/carers where necessary |

**Monitoring and Evaluation**

A report on the policy, including a breakdown of incidents, will be presented to the Resources Committee annually.

**Date for review: March 2017**

# 1 Using the Internet

The school Internet access is designed expressly for student use and includes both internal (school) and external (LA) filtering. Whilst efficient, no filtering system is 100% reliable and staff and students are responsible for any inappropriate access gained under their user name and must not attempt to access material deemed to be inappropriate. E.g. Social networking sites, pornography, gaming, gambling, music downloads (this is not an exhaustive list).

Students will be taught in ICT and Life skills lessons what Internet use is acceptable and what is not and in all curriculum areas be given clear objectives for Internet use in lessons. When using the Internet in lessons, staff should guide students to on-line activities that will support their planned learning outcomes for that lesson. In ICT lessons students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

## 1.1 Evaluation of Internet content

The school will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.

Students will be taught to be critically aware of the materials they read and be wary of accepting its accuracy. They will be taught to acknowledge sources of information used and to respect copyright when using Internet material in their own work.

## 1.2 Web Filtering

The school will work with the LA to ensure that systems to protect students are regularly reviewed and improved.

- If staff or students discover unsuitable sites, the URL must be reported to the e-Safety coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF (Internet Watch Foundation) or CEOP (Child exploitation & online protection centre)

In the case of reported misuse by students, the incident will be investigated by the e-safety coordinator and sanctions may include loss of network or internet privileges, and in extreme cases seclusion or exclusion. Each case will be investigated under its own merits and parents/carers will be informed. Students involved will be interviewed by the e-safety coordinator and given individual advice and counselling about e-safety. In cases of legality the schools Police Community Support Officer will be contacted to advise and support the school.

In the case of a child protection issue arising from use of the internet, the school's child protection officer will be informed and action taken in accordance with the school's Child Protection Policy. As far as possible the hardware concerned with the issue will be held in a safe place as possible evidence.

In the case of reported misuse by staff the incident will be investigated in accordance with normal staff disciplinary procedures.

## 1.3 Authorisation to use the Internet

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- All staff must read and sign the 'Staff ICT Acceptable Use Agreement' (attached Appendix 3) before using any school ICT resource.
- All staff who wish to use You Tube must sign a separate agreement (attached Appendix 4)
- Students must apply for Internet access individually by agreeing to comply with the computer/Internet agreement and e-safety rules and signing the agreements sent home. (attached Appendix 1 & 2)
- Parents will be asked to sign and return a consent form for student access to the internet. (From September 2010 this will be posted to parents and records of returns kept on file)

## 1.4 Parent Gateway

- Parents, Carers and staff who wish to use the Parent Gateway (to access SiMs data) are asked to sign an e portal usage policy before they are granted access (attached Appendix 5).

## 1.5 Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Brighton & Hove Council can accept liability for the material accessed, or any consequences resulting from Internet use. This is clearly stated in the parental consent form.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

## 1.6 Management of social networking personal publishing (see Appendix 7 Social Networking Policy for Patcham High School)

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Students will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location. E.g. House number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers will be advised not to run social network spaces for student use on a personal basis and not to allow contact with past or present students on face book or any other social networking site.

- Students will be advised on security when using social networking sites at home and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Students are told that bullying via social networking sites or other electronic communication is unacceptable and will be treated with the utmost seriousness by the school.
- Advice on the safe use of the internet and social networking sites will be offered in the form of a workshop to parents/carers annually and via the school web site. Parents will be advised that the school cannot be held responsible for incidents of bullying and harassment which take place out of school hours using home devices and advised that they should seek redress through the police.
- Cyber bullying will be dealt with in accordance with the school's bullying policy when incidents spill over into the school day. It is however the responsibility of parents/carers to ensure that their children are adopting safe practices at home when using ICT technology, including mobile phones and the internet.

## 1.7 Email

- The school will provide personal email accounts to both staff and students.
- All users of email should be aware that by using a school email address, the contents of these messages can and will reflect on the school. As such, messages should never be sent which could reflect badly on the school.
    - Should any messages of this nature be sent, access to the email system will be revoked and a sanction put in place by the e-safety coordinator in line with the behaviour for learning policy.
    - Emails should be sent, while keeping in mind that written communication can be interpreted differently by others, and every effort should be made to ensure any correspondence reflect the polite, professional attitude which we expect any member of our school to uphold.
- The primary use of address provided by the school is educational and should not be used for personal/private use or gain.
- Any correspondence between staff and students should take place through official email addresses and not personal ones. This is to ensure the protection of both our staff and students.
- Students must adhere to the 'Student Email Agreement – as written by the Digital Leaders' – Appendix 6.
- Students may only use approved e-mail accounts.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and will be restricted.
- All users must be aware of 'netiquette' when using e-mail. Users should ensure that e-mails are prepared with the same amount of care as any other form of communication and certainly never sent in haste.
- E-mail should not be considered a private medium of communication whilst in school
- All electronic mail originating, arriving, or in transit through any electronic mail system belonging to the school/council is the property of the school/council.

# 2 Management of published content on the school web site

The contact details on the website should be the school address, e-mail and telephone number. Individual staff school e-mail addresses will be published to aid communication. Staff or students' personal information will not be published.

The ICT Coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Employees should be aware that, in general, the employer retains intellectual property rights to all material (including software development) that is created by employees as part of their work. In certain circumstances the intellectual property rights may be shared, if an agreement to this effect is drawn up prior to such particular work being developed. (Copyright, Design & Patents act 1988)

## 2.1 Publishing of student images

- Images that include students will be selected carefully and be appropriate for use.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Permission for students whose images are published by the school will be check against the consent form for Parents and Carers (see Appendix 2).
- Written permission from the school should be obtained before students or parents/carers publish images taken from the school website or of school events.
- Work can only be published with the permission of the student and parents (see Appendix 2).

## 2.2 Use of cookies

Following a voluntary EU-ICO (e-Privacy Directive) Cookie Audit, we have revised the Privacy Policy to detail our renewed compliance with new and existing legislation.

Patcham High School's Website (patchamhigh.brighton-hove.sch.uk) uses Cookies to enhance the user's experience, as required by EU Legislation, we notify all users of this fact on each and every page. Like many other websites in the sector we assume that ***use of the website*** is agreement enough to store the cookies in question.

Our cookie audit revealed all cookies stored on users PC's are necessary and not invasive of privacy.

Cookies stored by Patcham High could contain but are not limited to, sensitive personal data, user names, passwords, addresses or contact details, and are likely to also contain an amount of website data such as photographs and text excerpts.

Patcham High (as a *web entity*) will take all necessary steps to ensure that highly sensitive data, including that which may be stored in cookies is communicated through encrypted means, but acknowledges that in some cases encryption may be impractical or not possible, if such a case ever arises the user will be notified.

If you would like to learn more about cookies read the ICO Guidance page at https://ico.org.uk/for-organisations/guide-to-pecr/cookies/

Patcham High School does not store, retain log or capture any Traffic or Location data from its user(s), however Patcham High cannot take responsibility for the practices of websites or services linked on its website. User discretion is advised and responsibility must fall with the user for Internet activity offsite. As a school we will never use third party advertisers on our website, and all personal data you provide us with will be held only by us.

You can chose to opt-out of cookie storage by adjusting your browser settings to reflect this wish. For guidance on how to achieve this please refer to the user guidance of your personal web browser.

# 3 Managing Information Systems

## 3.1 Information system security

- The schools server will be backed up to an off-site location each night
- Anti-Virus protection will be updated regularly.
- The security of individual staff and student accounts will be reviewed regularly.
- The administrator account password will be changed if it becomes known.
- Computers (including mobile devices) may not be connected to the school network either physically or wirelessly without specific permission
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Personal data will not be stored on school servers without specific permission. Files held on the school's network will be regularly checked.
- Software must not be installed or removed from computers without specific permission. All software used in school must be appropriately licensed for use.
- Staff and students will not leave their computers unattended without locking the work station nor share their passwords with others.
- Users must not use the school network to create or transmit or view offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Users must not engage in activities with any of the following characteristics:
    - wasting network resources
    - corrupting other users' data
    - violating the privacy of others
    - disrupting the work of others
    - using the network in a way which denies service to others
    - introducing viruses or hacking applications

# 4 New and Emerging Technologies

At Patcham we recognise the growing area of new and emerging technologies and the beneficial impact these can have on learning. As a school we strive to embrace these technologies where they can prove to be beneficial to our staff and students, and actively seek to create a culture of innovation amongst the staff in their approach to the planning and delivery of lessons. We recognise

that the breadth of new and emerging technologies is vast and difficult to individually define. As such when discussing these technologies we will define new and emerging technology as:

*'Innovative technology that is reshaping the nature of education. Computer and network based technologies which hold great potential for increasing the access to information as well as a means of promoting learning. Technologies which allows the transformation of classrooms into more engaging, collaborative and productive learning environments in which learning can be customised to students' specific needs, interests and learning styles; which allow the role of the teacher to move away from being the sole source of information to being a guide, facilitator and coach in the learning process.'*

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will be issued with a school phone where contact with students is required. E.g. on school trips.

## 4.1 Use of Video and Voice over IP (VVoIP)

At Patcham we are aware that the use of VVoIP technology is an effective way to enrich learning and help students engage and communicate with parties that they may otherwise not have access to. This technology has superseded video communication tools which were previously used within the school.

### 4.1.1 Users of VVoIP

- Students should ask permission from the supervising adult before making or answering a VVoIP call.
- Content of VVoIP communication should be monitored appropriately and be suitable for the students' age.
- Parents/guardians should have consented to students participating in filming/photography (see Appendix 2)
- Use of VVoIP outside of school time should be arranged through official contact details (school email addresses) and should only take place with multiple participants when students are involved. Where this is not possible a recording should be taken of the VVoIP session and stored.

### 4.1.2 Content

- When recording a VVoIP session the responsible adult should check to ensure that permission has been given for students to participate in filming/photography to be used at school (see Appendix 2)
- Recorded material should be stored securely to all review for at least 6 months
- When using third party material the teacher should check to ensure that recording is acceptable and does not breach intellectual property rights
- Supervising adult should ensure that content is age appropriate before engaging with a VVoIP call with off-site parties.

### 4.1.3 Social Media

This section applies in addition to Appendix 7: School Networking Policy. As a school we recognise the growing trend in using social media and the impact this can have on communication channels between staff, students and guardians. In order to support our staff in using these channels, staff must ensure the following:

- All social media accounts should be registered with the e-safety coordinator.
- Any users of official school accounts must realise that any communication broadcast in this format enters a public forum and must ensure the following:
    - Messages must be presented in a positive and professional context
    - Private messages between staff accounts and students accounts will be prohibited in order to help protect both our students and staff
    - Students must never be allowed to post comments using official school accounts; the member of staff in charge of supervising the account must approve any communication.
    - No information of a confidential or sensitive nature should be shared via social media.
    - No student names or links to students' personal social media accounts should be posted online.
    - Where photos are used these must be suitable for purpose and should not be used in association with student names or other information which may lead to students being personally identified.
    - If a staff member is unsure if the content of a communication would be suitable they must first seek approval from the Assistant Head in charge of Communication.
    - Staff accounts will be registered and linked to from the school website to allow transparency and ease of access for all stakeholders.

## 5 Use of Wifi

Use of the school WiFi will be subject to both guidelines governing the use of internet/network and own device agreements.

## 6 Students' own devices

- Students are permitted to bring mobile phones to school
- Students are expected to have devices switched off and out of sight during lessons (see Appendix 1) unless they have been asked to use them for educational purposes or as their journal or as directed by their teacher.
- Staff are expected to model the policy by not using mobile phones for personal reasons during lesson time
- The use of mobile phones by students will be at the discretion of the teacher and only to support learning. The sending of abusive or inappropriate text messages is forbidden.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues) is the responsibility of the user.
- Students must check their personal ICT device daily to ensure the device is free from unsuitable material and free from viruses etc. before bringing the device into school.
- Students must check their personal ICT device daily for basic Health and Safety compliance to ensure it is free from defects. Particular attention should be paid to the power lead (lead not frayed; plug correctly fitted and containing the correct fuse rating), the keyboard (all keys

present; no bare metal exposed), the screen (free from flicker and damage) and the device battery (able to hold a charge). Any personal ICT device that has obvious Health and Safety defects should not be brought into school.

- Parents/guardians should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal ICT device in the event of loss/damage to the device.

## 6.1 Acceptable use of students' devices

- The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons should only take place after permission has been given from a teacher or other member of staff
- Students are permitted to connect to the student 'BYOD' wireless service while using a personal ICT device in school once the consent form for WiFi has been signed by a parent/guardian (see Appendix X)
- There are no secure facilities provided at school to store personal ICT devices. Students should therefore keep their personal ICT device with them at all times.
- The school accepts no responsibility for any device owned by students, and any damage, loss or theft incurred while on school property or related off-site visits.
- Use of personal ICT devices during the school day is at the discretion of teachers and staff. Students must use devices as directed by their teacher.
- Playing games or other non-school work related activities are not permitted.
- Students shall make no attempts to circumvent the school's network security. This includes setting up proxies and downloading programs to bypass security.
- Students shall not distribute pictures or video or any other material relating to students or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

## 6.2 Consequences of misuse

- The procedures for staff in dealing with use of student devices in lessons are very clear and are shown in Appendix 6.
- The use of student devices which do not fall within the covered roles of Appendix 6 will be dealt with in line with the schools Behaviour Policy.

## 6.3 Protection of personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

# 7 Staff sharing of e-safety policy

- All staff will be asked to read this policy and its application and importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

# 8 Parental Involvement

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This will include parent evenings with demonstrations and suggestions for safe home Internet use and useful web sites on issues around the internet and e-safety will be posted on the school's web-site.

**APPENDIX 1**

## Student and parental agreements (sent to all parents by post)

Computer/Internet Agreement & Cyber Safety

**The school computer system provides Internet access to students. Following these simple rules will help protect students by clearly stating what is acceptable and what is not.**

1. I agree to keep my password secret and not allow other students to use my computer user name or password.

2. I agree to use the Internet only when my teacher asks me to. When using the Internet I will only access sites allowed by teaching staff.

3. I understand that if I use public chat rooms or social network sites, I should not divulge any personal details such as my name or address or agree to meet anyone and if I do I could be putting myself at risk. I understand that using privacy settings will keep my information private and not doing so will mean that anyone can see my personal web pages.

4. I agree to ensure that I take a back up of any important school work on a memory stick or other portable device.

5. I understand that if I have a mobile phone in school, that it should be switched off and out of site during lessons unless I am asked to use it as a learning tool or my journal. My phone should never be used to film, take a photograph or bully anyone else in school.

6. I agree to respect the computer equipment and protect it from both deliberate and accidental damage for the benefit of all the students in the school.

7. I understand that if I publish a web site to the Internet I am bound by laws of libel and will not publish information on the web that is libellous or slanderous to Patcham High School or any member of staff or student at Patcham High School.

8. I take responsibility for all material stored on my username. I will not store unnecessary images and music on the school network or VLE. All materials must be appropriate and relevant to my work as well as legal.
9. 
10. I understand that these rules apply to my use of the school computers at any time, including at lunchtime and after school.

11. I understand that failure to keep to the computer code will result in me being temporarily or permanently removed from the school network.

**Student's agreement**

I have read and understood the school rules for responsible computer and Internet use. I will use the computer system, Internet and my mobile phone in a responsible way.

**Signed**_____ **Date** _____

**APPENDIX 2**

# General Consent Form for Parents/Carers

**Please tick the box next to each statement as giving consent.**

-

☐ **Parent's consent for Internet Access**

I have read and understood the school rules for responsible Internet use and cyber safety and give permission for my son/daughter to access the Internet and the school VLE. I understand that the school will take all reasonable precautions to ensure that students cannot access inappropriate materials. I understand that the school or the local authority cannot be held responsible for the nature or the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. I understand that my child is responsible for any material accessed or stored on their user name and must keep their password and user name secure at all times. I understand that I am responsible for my child‟s use of the Internet at home. I agree that if my child mis-uses their mobile phone at school it may be confiscated.

✉ **Parent's Consent for Web and Print Publication of Student Work and Photographs**

I agree that, if selected, my son/daughter‟s work may be published on the school web site. I also agree that photographs and films that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

✉ **Filming in School.**

From time to time, to improve the quality of Teaching and Learning at Patcham we record lessons and this footage is only used within school to analyse how we can improve. If you have any objections to your child being in a lesson which is being filmed please contact the school.

Patcham High School students participate in a large number of projects and events inside and outside of school. In some cases a video may be made and I agree for it to be published on the website as long as it follows school rules that no student will be clearly identified.

**Signed**_____ **Date** _____

## APPENDIX 3

ICT Acceptable Use Agreement (Staff)

**All adults working with ICT equipment within Patcham High School must ensure that they have read and agree to abide by the Acceptable Use agreement**

**When using ICT equipment I will not:**

1. Give anyone access to my username or password
2. Open other people's files without express permission
3. Corrupt, interfere with or destroy any other user's information
4. Release any personal details of any colleague or student over the Internet
5. Reproduce copyright materials without the owner's permission and acknowledging the source
6. Use the school internet access for business, profit, advertising or political purposes
7. Forget to log out when I finish a session or to lock my computer when temporarily away from it

**When using e-mail I will:**

1. Observe "netiquette" on all occasions
2. Understand that e-mail should not be considered a private medium of communication whilst at school
3. Not include offensive, abusive or racist language in my message or any language which could be considered defamatory, obscene, menacing or illegal.
4. Make sure that nothing in messages could be interpreted as libelous
5. Not send any message which is likely to cause annoyance, inconvenience or needless anxiety

**When using the internet I will:**

6. Ensure that all web activities conform to the norms of moral decency
7. Watch for accidental access to inappropriate materials and report any offending site so that action can be taken.
8. Report any breaches of the Internet policy
9. Be aware that my use of the school network and internet facilities are monitored
10. Duly note, that for my own safety, I should not communicate with students or ex-students on social networking sites such as face book.

**I understand that copyright on work developed in school hours using school hardware and software remains the intellectual property of the school.**

**Declaration**

I have read and understood the Acceptable use of ICT/E safety Policy including the appendix Social Media Policy and the above Acceptable Use Agreement and agree to abide by all its conditions. I understand that if I am found to have contravened any of the requirements I may face disciplinary action.

Name (please print) ----------

Signed: ---------- Date: ----------

**APPENDIX 4**

# YouTube Acceptable Use Agreement (Staff)

**YouTube Access Agreement**

(Supplemental agreement)

YouTube access will be available on Teacher PCs only.

I have signed the standard Acceptable Use Agreement for Computer and Internet use in school.

I know who the e-safety coordinator is and the process of reporting inappropriate use or content.

I will not allow students to use YouTube on my login and will ensure that my computer is locked whenever I am away from it

I will ensure that content that is accessed via YouTube has previously been checked before displaying to students.

Name:

Signed:

Date:

**APPENDIX 5**

# PATCHAM HIGH SCHOOL PARENT GATEWAY POLICY

Please read this document, complete the form below and return to Patcham High School. We will then issue you with your username and password separately by email and text. If you do not have access to a computer and wish to 'Opt out' of the Parent Gateway please tick box below and return, as above.

**Patcham High School Parent Gateway Usage Policy**
This Policy applies wherever accessed through the Patcham High School Parent Gateway, whether the computer equipment used is owned by Patcham High School or not. The policy applies to all those who make use of Patcham HIgh's Parent Gateway.

**Ownership and Administration of this Policy**
Patcham High School owns and administers the policy. Capita Sims is responsible for managing Internet technology for Patcham High School; Capita SIMS manages the technology in compliance with the Policy.

**Security**
This Policy is intended to minimise security risks. These risks might affect the integrity of Patcham High's data, the Authorised Parent Gateway User and the individuals to which the Parent Gateway data pertains. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials to the Patcham High School Parent Gateway system by authorised users
- The wrongful disclosure of private, sensitive and confidential information
- Exposure of Patcham High School to vicarious liability for information wrongfully disclosed by authorised users

**Data Access**
This policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy are adhered to. This Policy aims to promote best used of the Parent Gateway system to further the communication and freedom of information between Patcham High School and Parent(s)\carer(s)

**Authorised Parent Gateway Users**
Patcham High's Parent Gateway system is provided for use only by persons who are Legally responsible for pupil(s) currently attending the school. Access is granted only on condition that the individual formally agrees to the terms of this Policy. The authorising member of school staff **must** confirm that there is a legitimate entitlement to access information for pupils the names of whom must be stated on the Parent Gateway Agreement and Policy Form.

A copy of the form will be held by the school for audit purposes. Requests for Access to the Parent Gateway system must be made to Patcham High School by returning the Agreement and Policy Form to Patcham High School , stating who the access is for and agreeing to abide by the rules of the policy.

**Personal Use**
Information made available through the Parent Gateway system is confidential and protected by law under the Data Protection Act 1998. To that aim:

- Users must not distribute or disclose any information obtained from the Parent Gateway system to any person(s) with the exception of the pupil to which the information relates or to other adults with parental

responsibility

- Users should not attempt to access the Parent Gateway system in any environment where the security of the information contained in the Parent Gateway system may be placed at risk e.g. a cybercafé; public computer; unsecured wireless networks.
- Users must never leave themselves logged into the Parent Gateway if there is the possibility of someone else using the computer, for instance, if they leave the room where the computer is placed they must close the Parent Gateway connection.

**Password Policy**

You must assume personal responsibility for your username and password. Never use anyone else's username or password. You must always keep your individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and user names should never be shared.

**Questions, Complaints and Appeals**

Parent Gateway users should address any complaints and enquiries about the Parent Gateway system to Patcham High by email: Parentsgateway@patchamhigh.co.uk or telephone: 01273 503908 Patcham High School reserves the right to revoke or deny access to the Parent Gateway system of any individual under the following circumstances:

- The validity of parental responsibility is questioned
- Court ruling preventing access to child or family members is issued
- Users found to be in breach of the Parent Gateway usage policy

If any child protection concerns are raised or disputes occur the school will revoke access for all parties concerned pending investigation.

**Please note**: Where Parent Gateway access is not available Patcham High School will still make information available according to Data Protection Act (1998) law.

Users are liable for potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

**Acceptance of the Patcham High School Learning Gateway Policy**

I_____parent/carer of_____In tutor group:_____

Please tick:

Confirm that I have read and accept the Patcham High School Parent Gateway Policy. I would like to be allocated a username and password to access the system.

Do not have access to a computer and therefore would like my child's/childrens' reports sent to my address.

Email Address _____

Signed_____Date_____

**APPENDIX 6**

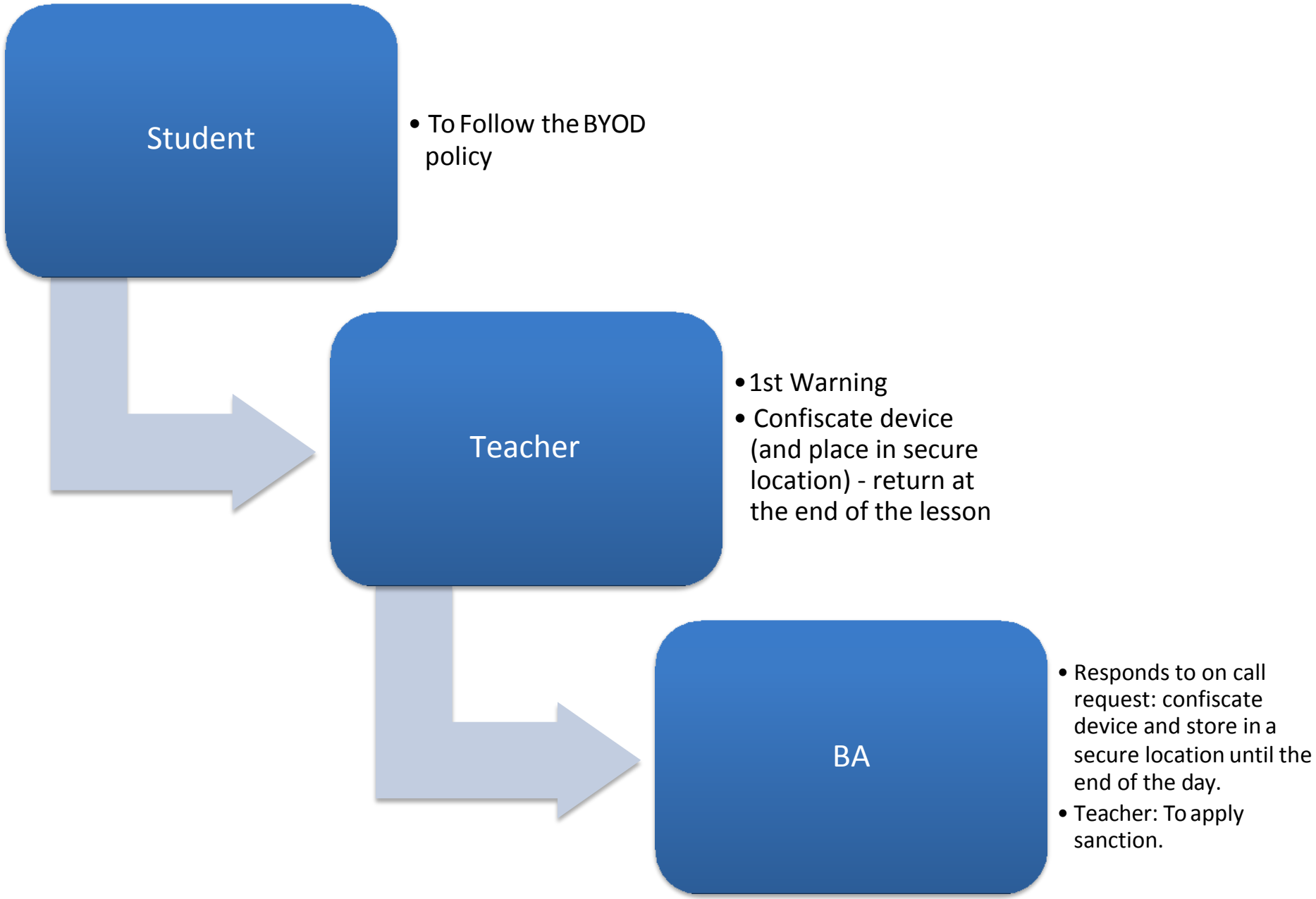
**Students' Own Device (BYOD) Agreement**

- Devices are brought into school at the owner‟s risk.
- Keep your password a secret and ensure your device is ‟locked „protected.
- Devices must on silent all the time.
- Devices can only be used in the classroom with the teacher‟s permission.
- Under no circumstances should photographs or videos be taken or shared on any device without consent.
- Student devices are not to be used to bully other members of the school community through any form of media.
- Failure to follow any of these rules may result in your device being taken from you.
- You will not attempt to circumvent the school‟s network security.

**Teacher Appendix**

- Ensure students follow the BYOD policy.
- If a student fails to comply with the policy
    - Give a warning
    - Ask for the device and place in a locked cupboard / drawer. Return the device to the student at the end of the lesson.
    - If a student fails to hand over their device, call a BA. The BA will take the device from the student and it will not be returned to them until the end of the day. The class teacher will apply a sanction.

Do not allow students to charge their devices in school




Reviewed March 2015 by Resources Committee

**APPENDIX 7**

# Social Networking Policy for Patcham High School

## 1. Introduction

1.1 The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people‟s lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

1.2 Whilst the widespread availability and use of social networking applications brings opportunities to engage and communicate with audiences in new and exciting ways, it is important to ensure that we balance this not only with our legal responsibilities to safeguard and protect our children and staff but also with the need to safeguard the school‟s image and reputation.

*1.3 The school E Safety Policy which includes a wider range of information on home and school ICT use, security & safeguarding issues (including how all school staff will be made aware of relevant issues and whom they should contact within the school if any concerns arise) should be read alongside this policy. See also Para. 9 below.*

## 2. Purpose

2.1 The purpose of this policy is to:

- support safer working practice by setting out the key principles and expected standards of behaviour when using social networking media
- ensure all children are safeguarded
- ensure the reputation of the school (its staff, pupils and governors at the school) are not damaged or compromised
- ensure that any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the School
- minimise the risk of misplaced or malicious allegations being made against those who work with pupils
- reduce the incidence of positions of trust being abused or misused
- ensure the school, its governors and staff are not exposed to legal risks.

## 3. Scope

3.1 This policy applies to the governing body, all teaching and other staff, whether employed by Brighton & Hove City Council or employed directly by the school, individual governors, external contractors providing services on behalf of the school or the City Council, teacher trainees and other trainees, supply staff, agency workers, volunteers and other individuals who work for, or provide services on behalf of, the school. These individuals are collectively referred to as „staff members‟ in this policy.

3.2 This policy cannot cover all eventualities and, therefore, staff members should consult the Headteacher if they are in any way unsure about what is and isn‟t acceptable use of social media.

## 4. Legal Framework

4.1 Patcham High School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of the law and professional codes of conduct.

4.2 Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School or Brighton & Hove City Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information.

4.3 Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media.

4.4 Patcham High School and Brighton & Hove City Council could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render the school or the County Council liable to the injured party.

## 5. Definition of Social Media

5.1 Social media is the term commonly used for websites which allow people to interact with each other in some way by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, Bebo and MySpace are perhaps the most well known examples of social media but the term also covers other web based services such as blogs, mircoblogs such as *Twitter*, chatrooms, forums, video and audio podcasts, open access online encyclopaedias such as *Wikipedia, message boards, photo document,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*.

5.2 This definition of social media is not exhaustive. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media. However, the principles set out in this policy must be followed irrespective of the medium.

5.3 For the purpose of this policy, the term social media also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

## 6. Principles - Social Media Practice

6.1 Staff members need to be aware that everything they post online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed and it is easy to lose control of it. They should therefore assume that everything they post online will be permanent and will be shared.

6.2 Staff members must be conscious at all times of the need to keep their personal and professional lives separate and to always maintain appropriate professional boundaries.

6.3 Staff members are responsible for their own actions and conduct and should avoid behaviour which might be misinterpreted by others or which could put them in a position where there is a conflict between their work for the school or Brighton & Hove City Council and their personal interests.

6.4 They must use social media in a professional, responsible and respectful way and must comply with the law, including equalities legislation, in their on-line communications.

6.5 Staff members must not engage in activities involving social media which might bring the school or the Council into disrepute.

6.6 They must not represent their personal views as those of the school or the Council on any social medium.

6.7 They must not discuss personal information about pupils, their family members, school or Council staff or any other professionals or organisations they interact with as part of their job on social media.

6.8 They must not name or otherwise identify pupils, former pupils or their parents, family members, colleagues etc in social media conversations.

6.9 They must not use social media or the internet in any way to attack, insult, abuse, defame or otherwise make negative, offensive or discriminatory comments about pupils, their family members, colleagues, other professionals, other organisations, the school or the Council.

6.10 They must not browse, download, upload or distribute any material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.

6.11 They must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

## 7. Personal Use of Social Media

7.1 Staff members need to be aware of the dangers of putting personal information such as addresses, home and mobile phone numbers, email addresses etc. onto social networking sites.

7.2 Staff members should ensure that they set the privacy levels of their personal sites at the maximum and opt out of public listings on social networking sites to protect their privacy.

7.3 Staff members should keep their passwords confidential, change them often and be careful about what is posted online. It is a good idea to use a separate email address just for social networking so that any other contact details are not disclosed.

7.4 Staff members should not identify themselves as employees of the school or Brighton & Hove City Council or service providers for the school or the City Council **in their personal webspace**. This is to prevent information on these sites being linked with the school or the Council. Where possible it may be useful to add a disclaimer such as "these are my own views and opinions and not those of my employer"

7.5 Taking the steps outlined in paragraphs 7.2 to 7.4 will avoid the potential for staff members to be contacted by pupils or their families or friends outside of the school environment and will reduce the chances of them becoming victims of identity theft.

7.6 All staff members should try to regularly review their social networking sites to ensure that information available publicly about them is accurate and appropriate. This should be suggested to new staff when they join the school. It is also good practice to close old accounts as they may contain personal information about you.

7.7 Staff members must not give their personal contact details including details of any blogs or personal social media sites or other websites to pupils or former pupils. It is also important to be aware that ex pupils may still have siblings in the school. Please refer to your schools own e-safety policy for more specific information. Please also see point 2.1 of this policy.

7.8 Staff members must not have contact through any personal social medium with any pupil, whether from this or any other school, unless the pupil is a family member or it is through school approved sites as part of official collaborative work. See point 7.11 below.

7.9 The school does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

7.10 It is strongly recommended that staff members do not have any contact with pupils" family members through personal social media. Please see point 6.1 & 6.2 above.

7.11 If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites.

7.12 Staff members must not establish, or seek to establish, social contact via social media/other communication technologies with pupils or ex-pupils and must never "friend" a pupil or ex-pupil through social media. These actions could be construed as being part of a "grooming process" in the context of sexual offending. This should be echoed in the school"s policy also. In the case of some social networking sites it is possible to be „followed" by a pupil without your consent. If this is the case, then your school should be informed and the pupil „follower" deleted.

7.13 Staff members must never use or access pupils" social networking sites.

7.14 Staff members must decline „friend requests" from pupils they receive in their personal social media accounts. If they receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become „friends" of the official school site or follow the school"s own policy.

7.15 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss or publish inappropriate information. Staff members must therefore make sure that they do not publish confidential information that they have access to as part of their employment on their personal webspace. This includes personal information about pupils, their family members, colleagues, Brighton & Hove City Council staff and other parties as well as school or City Council related information. This requirement continues after they have left employment.

7.16 Similarly, photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school or City Council uniforms or clothing with school or City Council logos or images identifying sensitive school or Council premises (e.g. care homes, secure units) must not be published on **personal webspace**.

7.17 The school or Council"s corporate, service or team logos or brands must also not be used or published on personal webspace.

7.18 Staff members must not use school or City Council email addresses and other official contact details for setting up personal social media accounts or for communicating through such media.

7.19 Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer"s IP address and the intervention will, therefore, appear as if it comes from the employer itself.

7.20 Staff members are advised to be cautious about inviting work colleagues to be „friends" in personal social networking sites. Social networking sites blur the line between work and personal lives and this may make it difficult to maintain professional relationships or embarrassing if too much personal information is known in the work place.

7.21 On leaving Patcham High School's service, staff members must not contact Patcham High School"s pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

## 8. Breaches of the Policy

8.1 Any breach of this policy may lead to disciplinary action, including the possibility of dismissal being taken against the staff member/s involved in line with Patcham High School or Brighton & Hove City Council"s Disciplinary Procedure.

8.2 Contracted providers of Patcham High School or Brighton & Hove City Council services must inform the Headteacher immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the

damage to the reputation of the school and the Council. Any action against breaches should be according to contractors‟ internal disciplinary procedures.