**Carshalton Boys Sports College**

| | |
|---|---|
| Policy | **Online Safety** |
| Policy Number: | PS03 |
| Review Date: | July 2017 |
| Approved by the Governing Body Committee: | |
| Next Review Date: | January 2018 |

# Contents

**Carshalton Boys Sports College Online Safety Policy**

## Development / Monitoring / Review of this Policy

This policy has been developed by a working group made up of:

- Paul Avery, Deputy Principal and Designated Safeguarding Lead
- Philip Brittain, Assistant Principal and Director of Technology
- Teachers and Support Staff
- Governors

## Schedule for Development / Monitoring / Review

| | |
|---|---|
| This policy was approved by the Governing Body on: | |
| The implementation of this policy will be monitored by: | *Paul Avery, Deputy Principal*<br>*Philip Brittain, Assistant Principal* |
| Monitoring will take place: | *Annually* |
| The Governing Body will receive a report on the implementation of this Policy: | *Annually* |
| This Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | *January 2018* |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Surveys / questionnaires of
    - students
    - parents / carers
    - staff

## Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

## Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

### Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Designated Safeguarding Lead
- regular monitoring of online safety incident logs
- reporting to relevant Governors meetings

### Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead.
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal is responsible for ensuring that the Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Designated Safeguarding Lead.

### Designated Safeguarding Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing this policy.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.
- Provides training and advice for staff.
- Liaises with the Local Authority / relevant body.
- Liaises with school technical staff.
- Creates a log of online safety incidents to inform future online safety developments.
- Meets regularly with Online Safety Governor to discuss current issues and review online safety incident logs.
- Attends relevant Governors meetings.

- Reports regularly to Senior Leadership Team.

### IT Manager

The IT Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

### Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy Agreement
- they report any suspected misuse or problem to the Principal or Designated Safeguarding Lead for investigation / action / sanction
- all digital communications with students and parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and Student Acceptable Use Policy Agreement
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### Students / Pupils:

- are responsible for using the school systems in accordance with the Student Acceptable Use Policy Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- are expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and the school website. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to school systems including access to student records
- their children's personal devices in the school (where this is allowed)

**Policy Statements**

### Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student Acceptable Use Policy Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

### Education – Parents / Carers

Many parents / carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the child's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, the school web site
- Parents Information Evenings
- High profile events / campaigns e.g. Safer Internet Day

### Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policy Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff.
- The Designated Safeguarding Lead will provide advice / guidance / training to individuals as required.

### Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are involved with online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

### Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.

- All users will be provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password regularly.
- Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### Mobile Technologies (including BYOD/BYOT)

Mobile devices may be school owned or personally owned and might include: smartphones, tablets, Chromebooks / notebooks / laptops or other technologies that usually have the capability of utilising WiFi networks. These devices will have access to the wider internet which may include cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

### Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be

published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Students' work can only be published with the permission of the student and parents / carers.

### Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Carshalton Boys does ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data

- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly logged-off at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

### Communications

When using communication technologies the Carshalton Boys considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, etc.) must be professional in tone and content.
- Users should adhere to generally accepted principles of email etiquette, as detailed in the appendices.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

### Social Media - Protecting Professional Identity

Schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment including legal risk.

Carshalton Boys staff should ensure that:

- No reference should be made in social media to students, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

When official school social media accounts are established there should be:

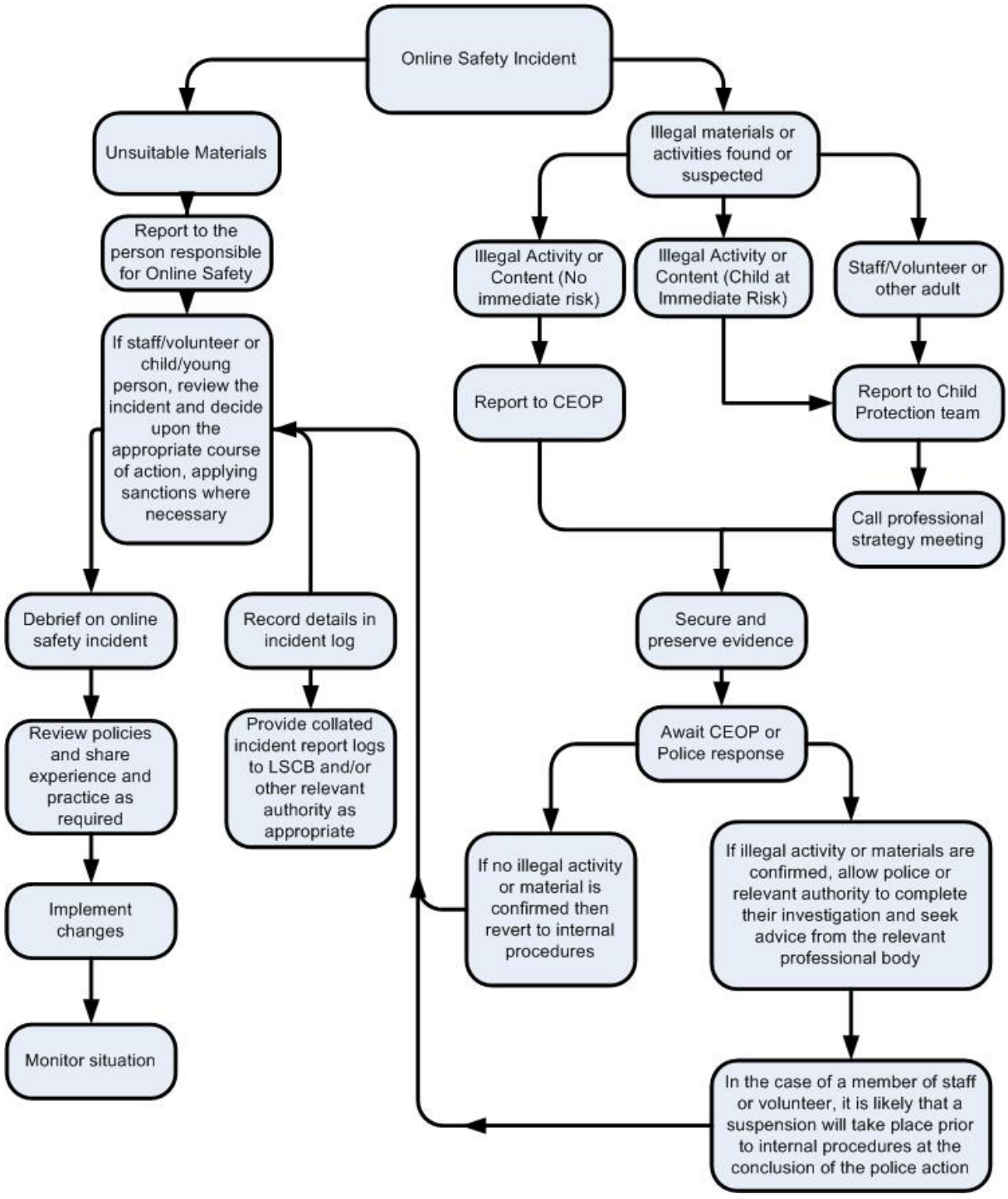
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

## Responding to illegal incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below) for responding to online safety incidents and report immediately to the police.



### Responding to other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

### School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

**Appendices**

## STAFF AND VOLUNTEERS ACCEPTABLE USE POLICY AGREEMENT

**School Policy**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff and volunteers to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff and volunteers are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technologies to enhance their work, to enhance learning opportunities for students and will, in return, expect staff and volunteers to agree to be responsible users.

**Acceptable Use Policy Agreement**

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school systems and devices are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge or express permission.
- I will communicate with others in a professional manner, including adhering to the generally accepted principles of email etiquette.
- I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless I trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions, both in and out of school:

- I understand that this Acceptable Use Policy Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

**Staff and Volunteers Acceptable Use Policy Agreement Form**

This form relates to the Staff and Volunteers Acceptable Use Policy Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy Agreement.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: …….

Signed: …….

Date: …….

## STUDENT ACCEPTABLE USE POLICY AGREEMENT

**School Policy**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy Agreement is intended to ensure that:

- Young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Young people are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

**Acceptable Use Policy Agreement**

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.).
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will treat school equipment with respect, as if it were my own, and never intentionally damage any equipment.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, including adhering to the generally accepted principles of email etiquette.
- I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones, USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Student Acceptable Use Policy Agreement Form**

This form relates to the Student Acceptable Use Policy Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy Agreement. If you do not sign and return this form, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own devices out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student:…..…….

Tutor Group:……...…….

Signed:…….…….

Date:…….

## EMAIL ETIQUETTE

The following guidelines have been derived from generally accepted principles of email etiquette. Users of the school email system are encouraged to heed this advice. Bear in mind that your emails reflect you.

**Privacy**

Never put in an email anything you wouldn't write on a postcard. Remember that emails can be forwarded, so unintended audiences may get to see what you have written. Respect the privacy of others, and avoid disclosing private information without prior consent. This is particularly important for emails marked as personal, private or confidential and those containing legal disclaimers.

**"To"**

You should include only those recipients in the "To" field that you are expecting a response from.

**"Cc"**

The use of "Cc", otherwise known as 'courtesy copy', implies that the recipient wants, needs or has asked to be copied into the email. Anything else falls under the category of SPAM. Consider including a reason why recipients have been copied into the email, but do not expect a reply. Avoid playing politics with this field. Do not copy in third parties in an attempt to apply pressure or cause embarrassment, often referred to as a 'tweaking Cc'. It will almost certainly cause offence to the recipient, and lead to unnecessary ill feelings.

**"Bcc"**

Use "Bcc", otherwise known as 'blind courtesy copy', sparingly. Recipients that have been Bcc'd into an email will not be visible to other users. There may be a good reason to use it, such as to protect the privacy of recipients by not including their names or email addresses in the "To" or "Cc" fields. However for all other intents and purposes, it has the potential to backfire on the sender and affect personal trust.

**Subject**

Do not leave the subject field blank. Use a brief, concise and meaningful description of the contents or purpose of the email.

**Reply to all**

Consider whether everyone from the original email actually needs to see your response. Either remove recipients from the list as appropriate, or consider replying only to the sender instead.

**Reply & Forward**

If you reply to an email, and then "Cc" a third party that the original sender did not include, you need to be certain that the original sender will not be troubled by it. This is particularly important if the original email contained confidential or sensitive information or data. The same applies to the forwarding of emails. You should always respect privacy and confidentiality.

**Attachments**

Avoid using attachments unless absolutely necessary. Most mailboxes come with a size limit, and you run the risk of clogging up both your own and the recipient(s) mailboxes. For

internal recipients consider storing the necessary file(s) on a shared area, and providing a link or a description of the location. For external recipients consider using a cloud based storage system. However care should be taken with confidential or sensitive files.

**CAPS**

Avoid using CAPS at all costs. It is the email equivalent of shouting. IF YOU FIND YOU HAVE TYPED A LINE OF TEXT IN UPPERCASE CHARACTERS BY ACCIDENT, you should consider deleting it and starting again. For emphasis, consider the use of bold formatting or **asterisks**.

**Urgent**

Avoid the use of the word 'urgent' in emails, unless entirely necessary. It may be perceived as condescending by the recipient, and risks genuinely urgent emails from not be treated as such. Be gracious enough to leave the recipient of the email to make a decision as to the urgency of the subject matter and prioritise your message accordingly.

**Important**

As with the use of the word 'urgent', only mark emails as important if they truly are. Over usage may result in the adverse effect.

**Virus warnings**

Virus warnings received from others are often hoaxes. Never forward these types of emails to other recipients, especially if asked to by the sender. If you are concerned with the contents of the email or unsure, don't hesitate to contact a member of the IT department.

**Sending emails outside of work hours**

Staff should avoid sending emails to co-workers outside of work hours, especially those that encourage a response or an action to be completed before the workday has commenced. Carshalton Boys promotes a healthy work-life balance for all of its employees.

**Think before you send**

Avoid sending emails when you are upset or emotional. If you receive an email that you deem to be inappropriate, do not respond immediately if at all. If you feel the need to write something down, do so on paper or another electronic medium other than email. A face-to-face or telephone conversation may be more appropriate.

Take the time to check your email for inaccuracies before sending, and take particular note of the list of recipients to ensure the email reaches its intended audience. It is not possible to stop or recall an email once it has been sent. If you discover your message has been sent incorrectly, send an apology to the recipient and ask that they delete your message from their mailbox.

**Missed signals**

Irony, sarcasm, humour and other such nuances of verbal communication can be difficult to express in an email, and easily misunderstood or misinterpreted. If in doubt, leave it out.

**Be polite and courteous**

You should always make the effort to be polite and courteous. Be patient, and allow the recipient sufficient time to respond before sending them a reminder. Never say anything you would not say to the recipients face. Avoid 'flaming', in other words expressing anger or

humiliating someone needlessly by copying others in on complaints and criticisms about them.

**Inappropriate use of email**

Never send, reply to, or forward vulgar, abusive, libellous, racist, obscene, incendiary or defamatory emails. Apart from being offensive, they and you may be breaking the law.

## Useful Links – e-safety related

London Grid for Learning (LGfL): http://onlinesafety.lgfl.net

'SWGFL 360 degree safe' audit tool which enables schools to evaluate their own online safety provision: https://360safe.org.uk/

The 2016 Keeping Children Safe in Education statutory guidance depicts a flowchart on page 10, on what actions to take when there are concerns about a child. These processes should also be followed as appropriate, when staff have concerns about a child's online safety / concerns prompted by a child's behaviour online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526153/Keeping_children_safe_in_education_guidance_from_5_September_2016.pdf

Advice for practitioners (including school staff) provides detailed information as to what to do if there are concerns a child is being abused, by the Department of Education, UK Government: https://www.gov.uk/government/publications/what-to-do-if-youre-worried-a-child-is-being-abused--2

Sexting Guidance document by the UK CEOP, the Child Exploitation Command of the National Crime Agency (NCA). This document includes a Sexting response flowchart in Annex 1: https://www.thinkuknow.co.uk/Teachers/blog/Dates/2013/3/Sexting-in-schools-What-to-do-and-how-to-handle-it/

Appropriate filtering and monitoring guides for schools and education settings, by the UK Safer Internet Centre: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring

CEOP Safety Centre - for help, advice or to report an incident: http://www.ceop.police.uk/

The Professionals Online Safety Helpline, by the UK Safer Internet Centre: http://www.saferinternet.org.uk/about/helpline

CEOP offers one day training for professionals (paid Ambassador training) on online safety. https://www.thinkuknow.co.uk/teachers/training/paidtrainingDetails/

UK Safer Internet Centre advice and resources for teachers and professionals: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals and Online Safety Briefings from young people: www.onlinesafetylive.com

Childnet's Professional resources: http://www.childnet.com/teachers-and-professionals

Keeping Children Safe Online by the children's charity NSPCC and CEOP, is an online introductory safeguarding course for anyone who works with children: https://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

CEOP's online safety education programme called Thinkuknow: http://www.thinkuknow.co.uk/

Childnet (a non-for-profit organisation working in online safety): http://www.childnet.com/resources

UK Safer Internet Centre, (a coordinated partnerships of SWGfL, the Internet Watch Foundation and Childnet): http://www.saferinternet.org.uk/advice-and-resources/young-people

SWGfL and Common Sense Media, which includes curriculum mapping: http://swgfl.org.uk/products-services/esafety/resources/Digital-Literacy

Parent Zone, a not-for-profit organisation, offers Parents information to help understand the digital world and raise resilient children. They also offer training for teachers on how to engage parents: http://parentzone.org.uk/

Parent and Carer support from the UK Safer Internet Centre: http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers

Childnet, provides information and advice for parents and carer, including a printable sheet available in 12 languages: http://www.childnet.com/resources/supporting-young-people-online

Vodafone's Digital Parenting resources: http://www.vodafonedigitalparenting.co.uk

Netware by NSPCC and O2, offers a guide to social networks for parents. https://www.net-aware.org.uk

Share Aware by NSPCC and O2, offers advice to parents about the internet: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware

Parentinfo by CEOP and Parent Zone provides high quality information to parents and carers: http://parentinfo.org

Parents section of CEOP's Thinkuknow website. https://www.thinkuknow.co.uk/parents/

Engaging parents with online safety by Kent Country Council: http://www.kelsi.org.uk/__data/assets/pdf_file/0004/29749/Engaging-Families-schools-and-professionals.pdf