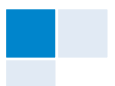




West Sussex Alternative Provision College



E-SAFETY POLICY



Contents:	<u>Page</u>
PART 1	
Introduction	4
Purpose	4
Scope	5
Roles and Responsibilities	5
e-Safety Complaints Procedures	6
Training	7
Summary	7
A. Managing the Internet Safely	9
B. Policy Procedures for Teaching and Learning	11
C. Education Programme	15
D. Email Safety	18
E. Digital Images	21
F. Use of Network	24
G. Cyber Bullying	26
H. Safeguarding Issues	27
I. Infringement Handling	28
J. Data Security	31



PART 2 – ACCEPTABLE USE	Page
Acceptable Use Policy	34
Staff Acceptable Use Policy	38
Staff User Agreement Form	42
Pupil Acceptable Use Policy KS1-KS2	43
Pupil User Agreement Form KS1-KS2	45
Student Acceptable Use Policy KS3-KS4	46
Student User Agreement Form KS3-KS4	49
Laptop/Tablet Loan Agreement	50
Useful Links	52

ADOPTED BY WSAPC GB	
CREATED	08/10/09
REVIEWED	27/10/14
REVIEW DATE (annually)	September 2015



PART 1 – INTRODUCTION

This document should be read in conjunction with guidance found on the West Sussex Grid for Learning (E-Safety in West Sussex Schools)

'College' refers to any WSAPC Centre or venue throughout this document.

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

'One of the strongest messages I have received during my review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-Safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area...'

The e-Safety Policy has been produced by the West Sussex Alternative Provision College (WSAPC) with the above statement in mind, building upon West Sussex County Council Capita Partnership E-Safety Policy 2013 and Government guidance to safeguard and promote the use and access to ICT technologies by learners in our care.

The development and expansion of the use of ICT, and particularly of the Internet, has transformed learning in educational establishments. Whilst the Internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young learners. Some of these risks include:

- ✦ Access and/or illegal downloading of inappropriate materials
- ✦ Unauthorised access/loss/sharing of personal information
- ✦ Sharing/distribution of personal images
- ✦ Sexual/criminal exploitation
- ✦ Plagiarism and copyright infringement
- ✦ Cyber-bullying/inappropriate communication
- ✦ Excessive use which could impact on social and emotional development/learning
- ✦ Inability to evaluate the quality, accuracy and relevance of information accessed via the Internet.

PURPOSE

It is the duty of WSAPC to ensure that every child in its care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the physical buildings.

This policy document is drawn up to protect all parties – the students, the staff and WSAPC - and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.



The WSAPC wishes to create a safe e-learning environment which will assist in:

- ✦ raising the educational standards of pupils
- ✦ promote individual achievement
- ✦ support the professional work of staff

The 3 main elements to achieve this are:

- ✦ an effective range of technological tools
- ✦ well defined policies and procedures with clear roles and responsibilities
- ✦ an e-Safety education programme for all stakeholders

This policy should be adhered to in conjunction with other WSAPC policies, ie data protection, anti-bullying, code of conduct, safeguarding and child protection.

It should be noted that this policy applies to all staff, regardless of their place of work, ie placement at other educational establishments, in pupils' homes and when working from home. All WSAPC personnel are expected to comply with the E-Safety Policy, adhering to the additional guidelines introduced for remote workers to prevent WSAPC ICT technologies being compromised as a result of remote access.

SCOPE

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- ✦ The Internet
- ✦ Email
- ✦ Instant messaging, often using simple web cams
- ✦ Blogs (an on-line interactive diary)
- ✦ Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- ✦ Social networking sites
- ✦ Video broadcasting sites
- ✦ Chat rooms
- ✦ Gaming sites
- ✦ Music and video download sites
- ✦ Mobile phones with camera and video functionality
- ✦ Smart phones with email, web functionality and cut down 'Office' applications
- ✦ Gaming consoles linked to the Internet

ROLES AND RESPONSIBILITIES

E-Safety is recognised as an essential aspect of strategic leadership in WSAPC and the Senior Leadership Team, with the support of the Governing Body, aims to embed safe practices into the culture of WSAPC. The responsibility for e-Safety has been designated to the **ICT Development Manager**.



1. The ICT Development Manager is **Ian Morley**. The ICT Development Manager monitors e-Safety issues and reports regularly to the Senior Leadership Team. E-Safety policies and procedures are reviewed annually.
2. The Governing Body has an overview of e-Safety issues and strategies at the WSAPC and receives an annual report on policy developments.
3. All teachers are responsible for promoting and supporting safe usage of ICT technology in their classrooms, ensuring E-Safety procedures are maintained. Assistant Headteachers (Head of Centres) will monitor procedures and processes at their respective centres reporting to the Senior Leadership Team any concerns.
4. Assistant Headteachers (Head of Centres) are responsible for ensuring a 'no blame' culture is embedded into practise so pupils feel safe in reporting any bullying, abuse or access to inappropriate materials.
5. All staff should be familiar with the WSAPC e-Safety Policy, including:
 - ✦ Safe use of email;
 - ✦ Safe use of Internet including use of internet-based communication services, such as instant messaging and social medias;
 - ✦ Safe use of WSAPC network, equipment and data;
 - ✦ Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
 - ✦ Publication of pupil information/photographs and use of website;
 - ✦ E-Bullying/Cyberbullying procedures;
 - ✦ Their role in providing e-Safety education for pupils.
6. Temporary personnel may be used to cover absentees or training on a casual basis. Should temporary workers require access to ICT technology as part of their role, the manager responsible for their day to day supervision will be required to bring this policy and its contents to their attention.

Staff will be made aware of the Computer Misuse Act 1990 at induction and will be informed of possible legal action/dismissal if breach of the Act is proved.

E-SAFETY COMPLAINTS PROCEDURES

WSAPC will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a WSAPC computer or mobile device. Neither WSAPC nor West Sussex County Council (WSSC) can accept liability for material accessed, or any consequences thereof, of Internet access.

WSAPC learners and parents/carers will be referred to the E-Safety Policy at interview and will be informed of the complaints procedure and sanctions in the event of infringement. The attention of learners, parents/carers will be directed to the Computer Misuse Act 1990, whereby the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence. Parents/carers will be encouraged to work in partnership with staff to prevent Internet misuse occurring.

Sanctions available include:



- ✦ Interview/counselling by tutor/Assistant Headteacher (Head of Centre)/Co- Head Teacher of WSAPC;
- ✦ Informing parents or carers;
- ✦ Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework);
- ✦ Referral to WSCC/Police.

The Assistant Headteacher (Head of Centre) acts as first point of contact for any complaint in relation to both staff and learners of their respective Centre.

Any complaint about staff misuse is referred to the Co-Head Teacher of WSAPC. If the complaint is in connection with the Co-Head Teacher, misuse should be referred to the Governing Body.

- ✦ Complaints of cyber-bullying are dealt with in accordance with the Anti-Bullying Policy.
- ✦ Complaints related to child protection are dealt with in accordance with WSCC/WSAPC child protection procedures.

Failure to comply with the requirements of this policy by staff may result in disciplinary action being taken by WSAPC.

TRAINING

An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible use of technologies. Instruction will take place as part of the induction process for new staff prior to access of the WSAPC network, and refresher training will be implemented at each Centre on an annual basis.

Training for pupils will be discreetly delivered in all lessons with particular emphasis given to e-Safety within ICT and PSHE lessons.

All staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

SUMMARY

E-Safety affects everyone, pupils, families, WSAPC staff, WSAPC Governing Body and all other stakeholders. It is given the highest safeguarding priority within WSAPC.

WSAPC reserves the right to monitor the use of its ICT facilities/resources both during routine audits and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purpose for such monitoring includes:

- ✦ Greater productivity and efficiency;
- ✦ To ensure the security of the system and its effective operation;
- ✦ To ensure there is no unauthorised use of equipment;
- ✦ To ensure the smooth running of the WSAPC if an employee is absent for any reason and communications need to be checked;
- ✦ To ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment;



- ✦ To ensure inappropriate materials are not being accessed;
- ✦ To ensure there is no breach of confidentiality.



A MANAGING THE INTERNET SAFELY

1. Why is Internet Access Important?

- ✦ The Internet is an essential element in 21st century life for education, business and social interaction.
- ✦ ICT skills and knowledge are vital to access life-long learning and employment. ICT is now seen as a functional, essential life-skill along with English and mathematics.
- ✦ The statutory curriculum requires pupils to learn how to locate, retrieve and **exchange** information using technology including the Internet.
- ✦ All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information.
- ✦ The Internet can benefit the professional work of staff and enhances the school's management information and business administration systems.

2. The Risks

- ✦ The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.
- ✦ Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.
- ✦ In line with WSAPC policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'no blame', supportive culture if pupils are to report abuse.
- ✦ WSAPC also needs to protect itself from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening emails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984). WSAPC makes it clear to users that the use of WSAPC equipment to view or transmit inappropriate material is "unauthorised" and infringements will be dealt with; and ensures that all reasonable and appropriate steps have been taken to protect pupils. Reasonable steps include technical and policy actions and an education programme for pupils and staff, (and parents).



3. Technology

- WSAPC has up-to-date anti-virus, anti-spyware and anti-spamware software and approved firewall solutions installed on their network. To make sure rogue applications are not downloaded and hackers cannot gain access to the WSAPC's equipment or into users' files through internet use, staff and pupils should not be able to download executable files and software.
- Unfortunately, inappropriate materials will inevitably get through any filtering system. WSAPC will be vigilant and alert so that sites can be blocked. Conversely, sometimes appropriate websites need to be unblocked
- Pupils publishing to the internet on a class WSGFL, Edmodo or Moodle website removes the difficulties of pupils publishing on a publicly available website because this can be a safe, closed environment which only they will have access to via their username and password.

4. Policy Statements

WSAPC:

- Maintains broadband connectivity through the West Sussex Grid for Learning using in house and external technical support for maintenance.
- Works in partnership with WSCC to ensure any concerns about the system are communicated to Openhive so that systems remain robust and protect students;
- Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot download executable files such as .exe/.com /.vbs etc.;
- Utilises caching as part of the network set-up;
- Ensures the ICT Development Manager is up-to-date with Openhive services and policies;
- Ensures the ICT Development Manager checks to ensure that the filtering methods are effective in practice and that they activate the removal of access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Has network auditing software installed;
- Uses security time-outs on Internet access where practicable/useful;
- Uses individual log-ins for pupils and all other users;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure Openhive portal or Learning Platform.



B POLICY PROCEDURES FOR TEACHING AND LEARNING

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. Supervision is the key strategy. Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

1. Surfing the Web

Aimless surfing should never be allowed. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question “Why are we using the Internet?”

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. The experienced teacher will choose a topic with care, select the search engine and then discuss with pupils sensible search words, which should be tested beforehand.

Pupils do not need a thousand websites on weather. A small selection may be quite enough choice. Favourites are a useful way to present this choice to pupils. If teachers’ website selections for various topics are put on the WSAPC Edmodo site, access by pupils from home is made possible. There may be difficulties here. Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing, for example, to a pornographic one. Therefore, sites should always be previewed.

2. Search Engines

Some common Internet search options are high risk, for example ‘Google Image Search’.

3. Collaborative Technologies

There are a number of Internet technologies that make interactive collaborative environments available. Often the term ‘social networking software’ is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcasting (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop presentation skills, helping children consider their content and audience. However, they are high risk environments and it is essential that teachers use them carefully.

5. Video Conferencing

Webcams: are used to provide a ‘window onto the world’ to ‘see’ what it is like somewhere else. WSCC use E2bn conferencing for ‘flash meetings’. Staff wishing to use Internet webcams outside of the WSCC environment should be aware of, and follow LA advice.

Pupils can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to



adult material. In WSAPC adult sites would normally be blocked but teachers need to preview any webcam site to make sure it is what they expect before ever using with pupils.

The highest risks lie with streaming webcams (one-to-one chat/video) that pupils use or access outside of the school environment. Pupils need to be aware of the dangers.

6. Social Networking Sites

These are a popular aspect of the web for young people. Sites such allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these sites are public spaces where adults hang out. They are environments that should be used with extreme caution. WSAPC will block such sites. However, pupils need to be taught safe behaviour as they may well be able to readily access them outside of school.

7. Podcasts

Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as Edmodo.

8. Chat Rooms

Many sites allow for 'real-time' online chat. Again, children should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chat rooms.

9. Sanctions and infringements

WSAPC's Internet e-Safety/Acceptable Use Policy needs to be made available and explained to staff/Governors, pupils and parents, with all signing acceptance/agreement forms appropriate to their age and role. WSAPC has clear possible sanctions for infringements.

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on WSAPC computers, the matter should be referred at the earliest opportunity to the local police station. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.



10. Policy Statements

WSAPC:-

- ✦ Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- ✦ We use the Openhive filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- ✦ Staff preview all sites before use or only use sites accessed from managed 'safe' environments such as Edmodo;
- ✦ Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- ✦ Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;
- ✦ Informs users that Internet use is monitored;
- ✦ Informs staff and students that they must report any failure of the filtering systems directly to the ICT Development Manager.
- ✦ Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform;
- ✦ Only uses Openhive for pupil's own online creative areas such as web space and e-Portfolio;
- ✦ Only uses the Openhive service for video conferencing activity;
- ✦ Only uses approved blogging or discussion sites, and blocks others.
- ✦ Only uses approved or checked webcam sites;
- ✦ Requires pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an e-Safety acceptable use agreement form which is fully explained and used as part of the teaching programme;
- ✦ Uses closed simulated environments for email with Key Stage 1 pupils;
- ✦ Requires all staff to sign an e-Safety/acceptable use agreement form and keeps a copy on file;
- ✦ Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programmes;
- ✦ Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- ✦ Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-Safety acceptable use agreement form at time of their daughter's/son's entry to WSAPC;
- ✦ Makes information on reporting offensive materials, abuse/bullying, radicalisation etc available for pupils, staff and parents;



- Immediately refers any material we suspect is illegal to the appropriate authorities – WSCC/Police.



C. EDUCATION PROGRAMME

- 1.** Pupils may still occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring.
- 2.** Pupils need to know how to respond responsibly if they come across material that they find distasteful, uncomfortable or threatening. For example: to turn off the monitor and report the incident to the teacher or ICT Development manager for inclusion in the list of blocked sites.
- 3.** Pupils must learn to recognise and avoid risks online – to become 'Internet Wise'. To STOP and THINK before they CLICK.
- 4.** Pupils also need to be 'savvy' about what they read, hear and see. In the same way that the quality of information received via radio, newspaper and television is variable, everyone needs to develop skills in selection and evaluation of Internet –based information. Just because something is published in text or on-line does not make it fact. It's therefore important that any education programme links to activities to help pupils evaluate what is fact, what is fiction and what is opinion, and that pupils consider whether something is plausible or biased.
- 5.** Information literacy skills therefore need to be taught. These include skills to 'read' content (contextual clues including design, lay-out, text, use of images, links to and from the content), where the material originates from and how the content can be validated
- 6.** Pupils will be accessing reliable material but need to select that which is relevant to their needs, for instance to answer a homework question. Pupils should be taught research techniques including how to narrow down searches and how to skim and scan content.
- 7.** The philosophy of sharing information across the Internet has increased the risk of pupils infringing copyright and committing plagiarism (the theft of ideas and works from another author and passing them off as one's own). For older pupils, there are numerous 'essay bank' websites offering access to essays for free or for a fee, often encouraging students to submit their own works. Pupils should be aware of the issues around copyright and encouraged to look for copyright information on websites, so reinforcing their understanding of the importance this issue. They also need to be aware that plagiarism is not only cheating but where sufficient is copied, an illegal infringement of copyright also constitutes a criminal offence.
- 8.** Pupils also need to understand the dangers of using unfiltered web access outside WSAPC at a location where parental controls or filtering have not been enabled. Pupils should be encouraged never to chat through a website or over a webcam with people that they do not already know and trust in the real world and not to post details about themselves to a website or in a blog or message.
- 9.** Pupils need to know how to deal with any Cyber Bullying incidents.
- 10.** E-Safety must be built into schemes of work as appropriate, to ensure pupils are 'taught' safe behaviours and practice and WSAPC fosters a 'no blame' culture to ensure pupils feel able to report any abuse, misuse or inappropriate content.
- 11.** Parents have an important role in supporting safe and effective use of the Internet by pupils.



12. Policy Statements:

WSAPC:

- ✦ Fosters a 'no blame' environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable;
 - ✦ Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher.
 - ✦ Ensures pupils and staff know what to do if there is a cyber-bullying incident;
 - ✦ Has a clear, progressive e-Safety education programme throughout all Key Stages, built on national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
 - to STOP and THINK before they CLICK
 - to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
 - to discriminate between fact, fiction and opinion;
 - to develop a range of strategies to validate and verify information before accepting its accuracy;
 - to skim and scan information;
 - to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be;
 - to know some search engines/websites that are more likely to bring effective results;
 - to know how to narrow down or refine a search;
 - to understand how search engines work;
 - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - to understand 'netiquette' behaviour when using an online environment such as a 'chat'/discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
 - to not download any files – such as music files - without permission;
 - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
 - to have strategies for dealing with receipt of inappropriate materials.
- 13.** Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright/intellectual property rights;
- 14.** Makes training available annually to staff on the e-Safety education program;



- 15.** Runs a rolling programme of advice, guidance and training for parents, including:
- ✦ Information in safety leaflets;
 - ✦ demonstrations, practical sessions held at school;
 - ✦ suggestions for safe Internet use at home;
 - ✦ provision of information about national support sites for parents.



D. EMAIL SAFETY

Email is now an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed email use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects.

However, unregulated email can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Once email is available it is difficult to control its content.

The WSAPC does not encourage the use of personal email for college business. Please note, if you use a personal email account for WSAPC business, be aware that any information you send is being transmitted across the public Internet. You could also find that under Freedom of Information, or as part of an investigation, you would need to give others access to your personal account.

1. Technology

- ✦ Incoming and outgoing email can be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defense. WSAPC have an appropriate educational, filtered Internet-based email system through the West Sussex Grid for Learning provided by Openhive.
- ✦ All emails in the WSGFL system go through a filtering process for inappropriate language.

2. Procedures

- ✦ Email should not be considered private and WSAPC reserves the right to monitor email. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.
- ✦ Many students will have their own email accounts, such as the web-based Hotmail or G-mail, which they use widely outside college, usually for social purposes. If email accounts are not monitored there is the risk that pupils could send or receive inappropriate material. The use of personal email addresses, such as Hotmail, should be avoided by staff and pupils. Staff are required to use appropriate Openhive systems for professional purposes.
- ✦ Individual pupil emails such as janet.brown@wsgfl.uk which allow pupils to send and receive messages to and from the wider world, must be carefully allocated to appropriate situations. Whole-class or project WSGFL email addresses should be used to communicate outside the WSAPC community.

3. Education

- ✦ Pupils need to be made aware of the risks and issues associated with communicating through email and to have strategies to deal with inappropriate emails. This is part of the WSAPC's e-Safety and anti-bullying education programme.
- ✦ There are programmes that can be used with the youngest pupils that 'simulate' an Email system. This provides a useful environment to teach the



skills of sending and receiving an email with or without an attachment to very young pupils.

- ✦ Pupils need to understand good 'netiquette' style of writing, and appropriate email behaviour appropriate to their age.

4. Policy statements

WSAPC:

- ✦ Does not publish personal email addresses of pupils or staff on the WSAPC website. We use anonymous, work or group email addresses for any communication with the wider public.
- ✦ If one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law we contact the police.

Pupils:

- ✦ We only use WSGFL (currently OPENhive) emails with pupils.
- ✦ Pupils can only use the WSGFL email accounts on the college system.
- ✦ Staff can only use the WSGFL email accounts on the college system.
- ✦ Pupils are introduced to, and use email as part of the ICT scheme of work.
- ✦ Year R/1 pupils are introduced to principles of email through closed 'simulation' software.
- ✦ Pupils are taught about the safety and 'netiquette' of using email i.e.
 - not to give out their email address unless it is part of a WSAPC managed project or someone they know and trust and is approved by their teacher or parent/carer;
 - that an email is a form of publishing where the message should be clear, short and concise;
 - that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
 - they must not reveal private details of themselves or others in email, such as address, telephone number, etc;
 - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
 - the sending of attachments should be limited;
 - embedding adverts is not allowed;
 - that they must immediately tell a teacher/responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
 - not to respond to malicious or threatening messages;
 - not to delete malicious or threatening emails, but to keep them as evidence of bullying;



- not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' email letters is not permitted.
- ✦ Pupils sign the school Agreement Form to say they have read and understood the e-Safety rules, including email and it is explained how any inappropriate use will be dealt with.

Staff:

- ✦ Staff use WSGFL email systems for professional purposes;
- ✦ Access in WSAPC to external personal email accounts may be blocked;
- ✦ An email sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on college headed paper. It should follow the college 'house-style';
 - the sending of attachments should be limited;
 - the sending of chain letters is not permitted;
 - embedding adverts is not allowed;
- ✦ Staff sign the appropriate WSCC/WSAPC Agreement form to say they have read and understood the e-Safety rules, including email and it is explained how any inappropriate use will be dealt with.



E DIGITAL IMAGES

1. Developing Safe School Web Sites

- ✦ The WSAPC website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the college's website for information and it can be an effective way to share the college's good practice and promote its work.
- ✦ Procedures and practice ensure website safety.
- ✦ The Data & Communication Manager will oversee/authorise the website's content and check suitability. Delegated members of staff will be given authority to upload content into sections of the website.

2. Use of Still and Moving Images

- ✦ The first name and last name of individuals in a photograph are NOT used. This reduces the risk of inappropriate, unsolicited attention from people outside the school.
- ✦ When the pupil is named, do NOT use their photograph/video footage.
- ✦ When the photograph/video is used, do NOT name the pupil.
- ✦ When showcasing examples of pupils work use only first names.
- ✦ Only use images of pupils in suitable dress to reduce the risk of inappropriate use.
- ✦ In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, the Data Protection Act may cover photographs taken for official college use, which are likely to be stored electronically alongside other personal data. As such, pupils and students should be advised why they are being taken.
- ✦ Written parental permission must be obtained before publishing any photographs, video footage etc. of pupils on the WSAPC website or in a DVD. This ensures that parents/carers are aware of the way the image of their child is representing the school.

3. Procedures

- ✦ Only use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.
- ✦ Links to any external websites are thoroughly checked before inclusion on WSAPC website to ensure that the content is appropriate both to the WSAPC and for the intended audience. All links are checked regularly, not only to ensure that they are still active, but that the content remains suitable too.
- ✦ Text written by pupils is always reviewed before publishing on the WSAPC website, ensuring that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem



obvious, pupils' work is checked so that it doesn't contain any statements that could be deemed defamatory.

- ✦ It is ensured that WSAPC is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a trademark for which copyright permission has not been sought.
- ✦ When WSAPC website contains any guestbook, noticeboard or blog, they will be monitored to ensure they do not contain personal details of staff or pupils.
- ✦ When WSAPC website uses a webcam it will be checked and monitored to ensure misuse does not occur accidentally or otherwise.
- ✦ When showcasing college-made digital video work, care is taken to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
- ✦ Digital images - photographs and video clips - can now readily be taken using mobile phones. Extreme abuse is the so called 'happy slapping' incidents sent to others or posted onto a website, eg social media sites such as 'YouTube'. It is therefore important to ensure that the risk of inappropriate use is minimised.
- ✦ Staff are advised not to use their personal phone or camera without permission e.g. for a college field trip. If personal equipment is being used it should be registered with the college and a clear undertaking that photographs will be transferred to the college network and will not be stored at home or on memory sticks and used for any other purpose than WSAPC approved business.

4. Technical

- ✦ Digital images/video of pupils need to be stored securely on the college network and old images deleted after a reasonable period, or when the pupil has left the WSAPC.
- ✦ Saved pictures must be in an image file that is appropriately named. Pupils' names must not be used in image file names or in <ALT> tag references when published on the web. *[An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers]*

5. Education

- ✦ Staff and pupils need to know who to report any inappropriate use of images to and understand the importance of safe practice.
- ✦ Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

6. Policy Statements

WSAPC

- ✦ The Data & Communication Manager has delegated overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;



- ✦ Uploading of information is restricted to the Business Administration team and overseen by the Data & Communication Manager and SLT;
- ✦ WSAPC web site complies with WSAPC's guidelines for publications;
- ✦ Most material is the WSAPC's own work; where other's work is published or linked to, sources are credited and the author's identity or status is stated clearly;
- ✦ The point of contact on the web site is the WSAPC central email and main telephone number. Home information or individual personal email identities will not be published;
- ✦ Photographs published on the web do not have full names attached;
- ✦ Parental/carer permission for use of digital photographs or video involving their child is agreed in writing prior to publication on the website;
- ✦ Parental/carer permission for internal use of digital photographs or video involving their child is authorised via the WSAPC agreement form when their daughter/son joins the WSAPC and is reviewed annually;
- ✦ Digital images/video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- ✦ Pupil names are NOT used when saving images in the file names or in the <ALT> tags when publishing to the WSAPC website;
- ✦ The full names of pupils are NOT included in the credits of any published WSAPC produced video materials/DVDs;
- ✦ Staff sign the college's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- ✦ Pupils are taught to publish for a wide range of audiences which might include governors, parents/carers or younger children as part of their ICT scheme of work;
- ✦ Pupils are taught about how images can be abused in their e-Safety education programme.



F. USE OF NETWORK

The computer system/network is owned by WSAPC and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The college reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

POLICY/PROCEDURE STATEMENTS

To ensure the network is used safely WSAPC:

1. Ensures staff read and sign that they have understood the WSAPC's e-Safety Policy. Following this, they are set-up with Internet and email access and can be given a network log-in username and password;
2. Ensures passwords for staff are a minimum of 8 digits containing both upper and lower case digits with at least one symbol or number
3. Provides pupils with an individual centre network log-in username. They are also expected to use a personal password containing at least one symbol;
4. Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
5. Makes clear that pupils should never be allowed to log-on without supervision or use/access via teacher and staff logins;
6. Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
7. Has set-up the centre network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
8. Requires all users to always log off when they have finished working or are leaving the computer unattended;
9. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
10. Ensures an automatic log off process is applied after a period of inactivity to secure the system in the event a computer is left unattended and logged on;
11. Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day. Curriculum computers and selected staff computers will be automatically closed down at 1900hrs each day;
12. Has set-up the network so that users cannot download executable files/programmes;
13. Has blocked access to music download or shopping sites – except those approved for educational purposes;
14. Scans all mobile equipment with anti-virus/spyware before it is connected to the network;



- 15.** Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the college provides them with a solution to do so;
- 16.** Makes clear that staff are responsible for ensuring that any computer or laptop/tablet loaned to them by the college, is used solely to support their professional responsibilities and that they notify the college of any “significant personal use” as defined by HM Revenue & Customs when required.
- 17.** Makes clear that staff accessing WSCC systems do so in accordance with any Corporate policies;
- 18.** Maintains equipment to ensure Health and Safety is followed in line with WSCC and WSAPC guidance;
- 19.** Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- 20.** Ensures that access to the WSAPC’s network resources from remote locations by staff is restricted and access is only through WSAPC/WSCC approved systems:
- 21.** Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- 22.** Provides pupils and staff with access to content and resources through the approved Learning Platform, Edmodo;
- 23.** Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent as a password protected attachment and in line with the WSAPC secure system for external communications;
- 24.** Follows WSCC advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- 25.** Reviews ICT systems regularly with regard to security.



G CYBER BULLYING

Students in WSAPC should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

1. **Cyber bullying** is bullying through the use of communication technology like mobile phone text messages, emails or websites. This can take many forms e.g.
 - ✦ Sending threatening or abusive text messages or emails, personally or anonymously
 - ✦ Making insulting comments about someone on a website, social networking site (eg: MySpace, Twitter, Facebook) or online diary (blog)
 - ✦ Making or sharing derogatory or embarrassing videos of someone via mobile phone or email (such as 'Happy Slapping' videos)
 - ✦ Abusive language or images used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the *Harassment Act 1997* or the *Telecommunications Act 1984*
 - ✦ Bullying is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against. It is intended to hurt the bullied emotionally and/or physically.

2. **This Links to WSAPC Anti-Bullying Policy and covers:**

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of college time:

- ✦ Advise the child not to respond to the message
- ✦ Refer to relevant policies including e-Safety/Acceptable Use, Anti-Bullying and PSHE and apply appropriate sanctions
- ✦ Secure and preserve any evidence
- ✦ Inform the sender's email service provider
- ✦ Notify parents of the children involved
- ✦ Consider delivering a parent workshop for the WSAPC community
- ✦ Consider informing the police depending on the severity or repetitious nature of offence
- ✦ Inform the WSCC e-Safety officer

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff:

- ✦ Inform and request the comments be removed if the site is administered externally
- ✦ Secure and preserve any evidence
- ✦ Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- ✦ Endeavour to trace the origin and inform police as appropriate
- ✦ Inform the Co-Head teacher who will inform the WSCC e-Safety officer



H SAFEGUARDING ISSUES

1. What are the E-Safety Issues?

- ✦ Although the use of ICT and the Internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.
- ✦ Apart from the risk of children accessing Internet sites which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways.
- ✦ It is known that adults who wish to abuse may pose as children to engage and then meet up with the children or young people they have been in communication with.
- ✦ This process is known as 'Grooming' whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones.
- ✦ An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.
- ✦ Increasingly bullying is conducted on the Internet or by the use of text messages and is therefore harder for schools to notice and deal with.
- ✦ Section 175 of the 2002 Education Act and Section 11 of the 2004 Children Act places upon all those who work with children a duty to safeguard and promote their welfare by creating a safe learning environment and where there are child welfare concerns, taking swift action to address them. **It is vital that WSAPC staff are aware of the signs which might indicate that a child is being groomed, bullied, radicalised or being subjected to inappropriate material and know how to take steps to begin to address this and safeguard and support the child.**

As with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for, but these can include: changes in children's behaviour, demeanour, physical appearance and presentation, language or progress.

2. If WSAPC staff are concerned that a child's safety is at risk because they suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

- ✦ Report to and discuss with the named child protection officer in WSAPC and contact parents
- ✦ Advise the child on how to terminate the communication and save all evidence
- ✦ Contact CEOP <http://www.ceop.gov.uk/>
- ✦ Consider the involvement of police and social services
- ✦ Inform the Co-Head Teacher who will notify the WSCC e-Safety officer



I INFRINGEMENT HANDLING

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of WSAPC management.

EXAMPLES

Pupils

Category A Infringements

- ✦ Use of non-educational sites during lessons
- ✦ Unauthorised use of email
- ✦ Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- ✦ Use of unauthorised instant messaging/social networking sites

Possible Sanctions: referred to class teacher/Assistant Headteacher (Head of Centre)

Category B Infringements

- ✦ Continued use of non-educational sites during lessons after being warned
- ✦ Continued unauthorised use of email after being warned
- ✦ Continued unauthorised use of mobile phone (or other new technologies) after being warned
- ✦ Continued use of unauthorised instant messaging/chatrooms, social networking sites, NewsGroups
- ✦ Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- ✦ Accidentally corrupting or destroying others' data without notifying a member of staff of it
- ✦ Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Possible Sanctions: referred to Class teacher/Assistant Headteacher (Head of Centre)/Co-Head Teacher/removal of Internet access rights for a period/removal of phone until end of day/contact with parent.

Category C Infringements

- ✦ Deliberately corrupting or destroying someone's data, violating privacy of others
- ✦ Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- ✦ Deliberately trying to access offensive or pornographic material
- ✦ Any purchasing or ordering of items over the Internet
- ✦ Transmission of commercial or advertising material

Possible Sanctions: referred to Class teacher/Assistant Headteacher (Head of Centre)/Co-Head Teacher/removal of Internet and/or Learning Platform access rights for a period/contact with parents/removal of equipment.



Category D Infringements

- ✦ Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- ✦ Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- ✦ Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- ✦ Bringing the WSAPC name into disrepute

Possible Sanctions – Referred to Co-Head Teacher of WSAPC/Contact with parents/possible exclusion/removal of equipment/refer to Community Police Officer/WSCC e-Safety officer (secure and preserve any evidence; inform the senders email service provider)

Staff

Category A Infringements (Misconduct)

- ✦ Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- ✦ Use of personal data storage media (e.g. USB memory sticks) without clearance/authorisation from the ICT Development Manager.
- ✦ Not implementing appropriate safeguarding procedures.
- ✦ Any behaviour on the world-wide-web that compromises the staff members' professional standing in the college and community.
- ✦ Misuse of first level data security, e.g. wrongful use of passwords.
- ✦ Breaching copyright or license e.g. installing unlicensed software on network

Sanction - referred to line manager/Assistant Headteacher (Head of Centre)/Business Manager. Account monitored by ICT Development Manager and warning given.

Category B Infringements (Gross Misconduct)

- ✦ Serious misuse of, or deliberate damage to, any WSAPC/WSCC computer hardware or software;
- ✦ Any deliberate attempt to breach data protection or computer security rules;
- ✦ Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- ✦ Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- ✦ Bringing the WSAPC name into disrepute.

Sanctions – Referred to Co-Head Teacher of WSAPC/Governing Body and follow WSCC disciplinary procedures; report to WSCC Personnel/ Human resources, report to Police – remove the PC to a secure place to ensure that there is no further access to the equipment; Instigate an audit of all ICT equipment by an outside agency to ensure that there is no risk of pupils accessing inappropriate materials in WSAPC. If a member of staff commits an exceptionally serious act of gross misconduct they



should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. In the case of child sexual abuse images being found, the member of staff will be **immediately suspended** and the Police should be contacted.

Staff and Pupils will be Informed of these Procedures by:

- ✦ They will be fully explained and included within WSAPC's e-Safety/Acceptable Use Policy. All staff will be required to sign WSAPC's e-Safety Policy acceptance form;
- ✦ Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'.
- ✦ Pupils will sign an age appropriate e-Safety/Acceptable Use form;
- ✦ WSAPC's e-Safety policy will be published on the website and made available and explained to parents/carers. Parents/carers will sign an acceptance form when their child starts at WSAPC.
- ✦ Information on reporting abuse/bullying etc. will be made available by WSAPC for pupils, staff and parents.



J DATA SECURITY

1. Ensure the protection of confidentiality, integrity and availability of WSAPC information and assets.
2. Ensure all users are aware of and fully comply with all relevant legislation.
3. Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

Definitions

Information - covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

Personal Data - Any data which can be used to identify a living person. This includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, email addresses and so on. It applies only to that data which is held, or intended to be held, on computers ('equipment operating automatically in response to instructions given for that purpose'), or held in a 'relevant filing system'. This includes paper filing systems.

Strong Password – Password which is 8 characters minimum length, contains upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain dictionary words, the owner's date of birth or car registration number.

Encryption – Process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Responsibilities

- ✦ WSAPC through WSCC shall be registered with the Information Commissioner's Office (ICO) under the 1998 Data Protection Act.
- ✦ Users of the WSAPC's ICT systems and data must comply with the requirements of the ICT Security Policy.
- ✦ WSAPC's Senior Leadership Team shall review this document at least annually.
- ✦ Users shall be responsible for notifying the ICT Development Manager/Business Manager and Co-Head Teacher of WSAPC of any suspected or actual breach of ICT security.
- ✦ **The Co-Head Teacher of WSAPC shall inform both the ICO and the Director of Learning, WSCC if there are any losses of personal data**
- ✦ Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- ✦ Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- ✦ Adequate procedures must be established in respect of the ICT security implications of personnel changes.



- ✦ No personal data shall be taken from WSAPC unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, netbooks, tablets, external hard disks, memory sticks and Personal Digital Assistants (PDAs) & other removable media.
- ✦ Remote access to information and personal data shall only be provided through an encrypted link and users shall require a strong password that is renewed at least termly.
- ✦ Users shall not publish spreadsheets, databases or other documents containing personal data on externally accessible web sites unless these documents are encrypted.
- ✦ Users shall not carry hard files containing sensitive data between sites/home/external establishments.
- ✦ Users shall not use memory sticks unless they are encrypted and authorised for use by the ICT Development Manager.

Physical Security

- ✦ As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- ✦ Server rooms must be kept locked when unattended.
- ✦ Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- ✦ All WSAPC owned ICT equipment and software should be recorded and an inventory maintained.
- ✦ Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.
- ✦ Computer screens should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
 - **Do not** leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
 - **Do not** give out sensitive information unless the recipient is authorised to receive it.
 - **Do not** send sensitive/personal information via email or post without suitable security measures being applied.
- ✦ Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security

- ✦ Users **shall not** make, distribute or use unlicensed software or data.
- ✦ Users **shall not** make or send threatening, offensive or harassing messages.
- ✦ Users **shall not** create, possess or distribute obscene material.



- ✦ Users must ensure they have authorisation for private use of WSAPC's computer facilities.
- ✦ Passwords should be memorised. If passwords must be written down they should be kept in a secure location.
- ✦ Users who regularly access personal data shall have a unique user ID and a strong password that is renewed at least termly
- ✦ Passwords **shall not** be revealed to unauthorised persons.
- ✦ Passwords **shall not** be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- ✦ Passwords shall be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- ✦ Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
- ✦ Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.
- ✦ Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection

- ✦ WSAPC should ensure current and up to date anti-virus software is applied to all WSAPC ICT systems.
- ✦ Laptop/tablet users shall ensure they update their virus protection at least weekly.
- ✦ Any suspected or actual virus infection must be reported immediately to the ICT Development Manager and that computer shall not be reconnected to the Centre network until the infection is removed.

Disposal of Equipment

- ✦ WSAPC shall ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.
- ✦ It is important to ensure that any software remaining on a PC being relinquished for reuse is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- ✦ WSAPC shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.



PART 2 - ACCEPTABLE USE POLICY

Networked resources, including Internet access, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the WSAPC. Any expression of a personal view about the WSAPC matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of WSAPC into disrepute is not permitted.

The WSPAC expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Independent pupil use of the Internet or the WSAPC's Intranet will only be permitted upon receipt of signed permission and agreement forms as laid out below. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using (see section 13.0 in the WSCC ICT in schools Acceptable Use Protocol guidance, accessed via the West Sussex Grid for Learning). Users will accept personal responsibility for reporting any misuse of the network to the ICT Development Manager.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

1. NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:




- a. Be polite – never send or encourage others to send abusive messages.
- b. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- c. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.



- d. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders.
- e. Password – do not reveal your password to anyone. If you think someone has learned your password then contact the ICT Development Manager.
- f. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
- g. Disruptions – do not use the network in any way that would disrupt use of the network by others.
- h. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
- i. Staff or students finding unsuitable websites through the college network should report the web address to the ICT Development Manager.
- j. Do not introduce floppy disks or “pen drives” into the network without having them checked for viruses prior to use.
- K. Do not attempt to visit websites that might be considered inappropriate (such sites would include those relating to illegal activity). All sites visited leave evidence in the WSAPC network if not on the computer. Downloading inappropriate material is illegal and the police or other authorities may be called to investigate such use.
- l. Unapproved system utilities and executable files will not be allowed in pupils’ work areas or attached to email.
- m. Files held on the WSAPC’s network will be regularly checked by the ICT Development Manager.
- n. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

2. UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

-  Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
-  Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
-  Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The WSAPC have filters in place to block emails containing language that is or may be deemed to be offensive.)



- ✦ Accessing or creating, transmitting or publishing any defamatory material.
- ✦ Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting (see section 8.0 in the WSCC ICT in schools Acceptable Use Protocol guidance accessed via the WSGFL).
- ✦ Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data (see section 9.0 respectively in the WSCC ICT in schools Acceptable Use Protocol guidance accessed via the WSGFL).
- ✦ Transmitting unsolicited material to other users (including those on other networks).
- ✦ Unauthorised access to data and resources on the school network system or other systems.
- ✦ User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

3. ADDITIONAL GUIDELINES

Users must comply with the acceptable use policy of any other networks that they access.

Users must not download software onto the WSAPC network without approval from the ICT Development Manager.

4. SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the WSAPC. The college will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

5. NETWORK SECURITY

Users are expected to inform the ICT Development Manager immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

6. PHYSICAL SECURITY

Staff users are expected to ensure that portable ICT equipment such as laptops, tablets, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.








7. WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the WSAPC system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

8. MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before photographs of pupils are published. Named images of pupils will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

-  the school website/VLE/Edmodo,
-  the WSCC website,
-  web broadcasting,
-  TV presentations,
-  Newspapers.

Pupils' work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.

Further details on Acceptable Use protocols can be found on the West Sussex Grid for Learning website.

Pupils who misuse or damage ICT resources will be subject to the stepped approach to behaviour management outlined in WSAPC Learning and Anti-Bullying policies.



STAFF ACCEPTABLE USE POLICY

WSAPC networked resources, including SIMs and Edmodo are intended for educational purposes, and may only be used for legal activities consistent with the rules of the College. If you make a comment about the College or County Council you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the WSAPC or WSCC into disrepute is not permitted.

All users are required to follow the conditions laid down in the Policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Conditions of Use

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to their Assistant Headteacher (Head of Centre) or the ICT Development Manager.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the WSAPC ethos and e-Safety Policy.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the WSAPC (or West Sussex County Council) into disrepute.
2	I will use appropriate language –I will remember that I am a representative of the WSAPC on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.



6	I will not trespass into other users' files or folders.
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the ICT Development Manager.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under other users username I will NOT continue using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera/smart phones for creating or transferring images of children and young people without the express permission of the WSAPC leadership team.
12	I am aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to a Co-Head Teacher and the ICT Development Manager/Business Manager
15	I will not use "USB drives", portable hard-drives, "floppy disks" or personal laptops on the network without having them "approved" by the WSAPC and checked for viruses.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
18	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such as WSAPC parents/carers and their children.
19	I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
20	I will support and promote the WSAPC's E-Safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.



21	I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held on the SIMS.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the WSAPC system.
24	I will ensure that portable ICT equipment such as laptops, tablets, digital still and video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.

Additional guidelines

- ✦ Staff must comply with the acceptable use policy of any other networks that they access.
- ✦ Staff will follow the "Safer Use Of The Internet By Staff Working With Young People" published within the West Sussex Schools Acceptable Use Policy - <http://wsgfl.westsussex.gov.uk/AUP>

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the WSAPC. The College will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the ICT Development Manager/Business Manager immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the WSAPCs network will be regularly checked by the ICT Development Manager. Users identified as a security risk will be denied access to the network.

MEDIA PUBLICATIONS

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.

Further guidance can be found in the West Sussex County Council "Model Policy for Schools regarding Photographic Images of Children" August 2010.



Copies can be obtained from section 6 of the WSSS Schools Acceptable Use Policy -

<http://wsgfl.westsussex.gov.uk/AUP>



STAFF USER AGREEMENT FORM FOR THE STAFF ACCEPTABLE USE POLICY

As a WSAPC User of the network resources, I agree to follow the College rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the College Acceptable Use Policy. If I am in any doubt I will consult the ICT Development Manager/Business Manager.

I agree to report any misuse of the network to the ICT Development Manager.

I also agree to report any websites that are available on the WSAPC Internet that contain inappropriate material to the ICT Development Manager

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

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



STAFF NAME	
STAFF SIGNATURE	
DATE	



PUPIL ACCEPTABLE USE POLICY (KS1-KS2)

All pupils must follow the rules in this policy when using WSAPC computers, and the college intranet.

Pupils that do not follow these rules may find:

-  They are not allowed to use the computers,
-  They can only use the computers if they are more closely watched.

Teachers or assigned Teaching Assistants will show pupils how to use the computers.

Computer Rules	
1	I will only use polite language when using the computers.
2	I must not write anything that might upset someone or give the college a bad name.
3	I know that my class teacher will regularly check what I have done on the college computers.
4	I know that if my class teacher thinks I may have been breaking the rules they will check on how I have used the computers before.
5	I must not tell anyone my name, where I live, or my telephone number over the Internet.
6	I must not tell my username and passwords to anyone else but my parents/carers.
7	I must never use other people's usernames and passwords or computers left logged in by them.
8	If I think someone has learned my password then I will tell my class teacher.
9	I must log off after I have finished with my computer.
10	I know that email is not guaranteed to be private. I must not send unnamed emails.
11	I must not use the computers in any way that stops other people using them.
12	I will report any websites that make me feel uncomfortable to my class teacher.
13	I will tell my class teacher or an adult in my classroom straight away if I am sent any messages that make me feel uncomfortable.



14	I will not try to harm any equipment or the work of another person on a computer.
15	If I find something that I think I should not be able to see, I must tell classroom teacher straight away and not show it to other pupils.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- ✦ Using a computer with another person's username and password.
- ✦ Creating or sending on the Internet any messages that might upset other people.
- ✦ Looking at, or changing work that belongs to other people.
- ✦ Waste time or resources on college computers.



PUPIL USER AGREEMENT FORM FOR THE PUPIL ACCEPTABLE USE POLICY (KS1-KS2)

I agree to follow the rules as detailed in the KS1-2 Acceptable Use Policy and explained to me by my classroom teacher when using a computer on a WSAPC Centre. I will use the network in a sensible way and follow instruction from classroom teachers and teaching assistants when using a computer.

I agree to report anyone not using the computers sensibly to my classroom teacher.

I also agree to tell my classroom teacher or an adult nearby if I see any websites that that make me feel unhappy or uncomfortable.

If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Student Name: _____

I realise that any pupil under reasonable suspicion of not following these rules when using (or misusing) the computers may have their access to computer equipment restricted or removed, more closely monitored or past use investigated.

PARENT/CARERS NAME	
PARENT/CARERS SIGNATURE	
DATE	



STUDENT ACCEPTABLE USE POLICY (KS3-KS4)

Pupil access to the West Sussex Alternative Provision network and intranet is a privilege, not a right. All pupils must follow the conditions described in this policy when using the college network, Internet access and the WSAPC Intranet

Pupils that do not follow these conditions may face:

- 🔹 Withdrawal of the access,
- 🔹 Monitoring of the network activity,
- 🔹 Investigation of past network activity,
- 🔹 In some cases, criminal prosecution.

Students will be shown how to use the resources available through the WSAPC network by their teachers. College staff will regularly check the network to make sure that it is being used responsibly.

The WSAPC will not be responsible for any loss of data or work as a result of the system or pupil mistakes in using the system. The use of any information gathered via the network and the school Internet connection is at the student's own risk.

Conditions of Use

Students will be expected to use the WSAPC network system for the purposes for which the college provides it. It is the personal responsibility of every student to take all reasonable steps to follow the conditions set out in this Policy. Students must also accept personal responsibility for reporting any misuse of the network to the Assistant Headteacher (Head of Centre), or a member of WSAPC staff.

Acceptable Use

Students are expected to use the network systems in a responsible manner. It is not possible to provide a complete set of rules about what is, and what is not, acceptable. All use however should be consistent with the college ethos and code of conduct. The following list does provide some examples that must be followed:

1	I will not create, send or post any material that is likely to: upset or offend other people or give the WSAPC (or West Sussex County Council) a bad name.
2	I will only use appropriate language – I will remember that I am a member of the college on a public system.
3	I will not use language that could stir up hatred against any ethnic, religious or other minority group.
4	I realise that members of staff will regularly check files held on the WSAPC network.
5	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
6	I will not trespass into other users' files or folders.



7	I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the Assistant Headteacher (Head of Centre), or a Teacher.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under other users username I will not continue using the machine – I will log it off immediately.
11	I understand that I will not be allowed access to unauthorised chat rooms and should not attempt to gain access to them.
12	I am aware that email is not guaranteed to be private. Messages supporting of illegal activities will be reported to the authorities. Anonymous/unnamed messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access to other people's information, unsuitable websites that make me feel uncomfortable to the Assistant Headteacher (Head of Centre) or a Teacher.
15	I will report to a Teacher or Teaching Assistant immediately if I am sent any messages or materials that make me feel uncomfortable.
16	I will not introduce "USB drives" or other portable devices into the network without having them approved and checked for viruses.
17	I will not try to visit websites that might be inappropriate or illegal. Downloading some material is illegal and I know the police or other authorities may be called to investigate if this were done.
18	I will not download or install any unapproved software from the Internet.
19	I realise that pupils under reasonable suspicion of misusing the network may have their usage closely monitored or have past use investigated. Illegal activities of any kind are strictly forbidden.
20	I will not receive, send or publish material that violates copyright law.
21	I will not attempt to harm any equipment, work of another user, or another website connected to the school system.
22	I understand that unapproved software and executable files are not allowed in my work areas or attached to emails.



23	I agree to follow the acceptable use policy of any other websites or networks that I access.
----	--

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- ✦ Logging in with another person's user ID and password, or using a machine left unattended, but logged in by another user.
- ✦ Creating, sending, or posting on the Internet any material (text, images or sounds) that is likely to upset other people, cause offence.
- ✦ Unauthorised access to resources and work that belong to other "users".
- ✦ Pupil activity that would cause:
 - Damage or destruction of other users' work,
 - Go against the privacy of other users,
 - Deliberately waste time or resources on the school network.

NETWORK SECURITY

If you discover a security problem, for example being able to see other students or staff work areas, you must inform the Assistant Headteacher (Head of Centre) immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

Please sign the Acceptable Use agreement attached to indicate your acceptance and understanding of this Policy.



STUDENT USER AGREEMENT FORM FOR THE STUDENT ACCEPTABLE USE POLICY (KS3-KS4)

I agree to follow the WSAPC rules on the use of the college network resources. I will use the network in a responsible way and follow all the conditions explained in the WSAPC Acceptable Use Policy.

I agree to report any misuse of the network to the Assistant Headteacher (Head of Centre) or a Teacher.

I also agree to report any websites that are available on the WSAPC Internet that contain inappropriate material to the Assistant Headteacher (Head of Centre) or a Teacher

I realise that any Student under reasonable suspicion of misusing the network may have their use monitored or past use investigated. If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other sanctions.

STUDENT NAME	
STUDENT SIGNATURE	
DATE:	
PARENT/CARERS NAME	
PARENT/CARERS SIGNATURE	
DATE	



WSAPC LAPTOP/TABLET LOAN AGREEMENT

It has been agreed that a laptop/tablet computer will be loaned to you while you remain employed at the WSAPC. This loan is subject to review on a regular basis, and can be withdrawn at any time.

As a member of staff to whom a laptop/tablet has been loaned I have read and agree to the following terms and conditions that apply while the laptop/tablet is in my possession:

- 1 The laptop/tablet, and any accessories provided with it, remains the property of WSAPC and is strictly for my sole use in assisting in the delivery of the Curriculum/Business Administration.
- 2 I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle. If the laptop/tablet is stolen from an unattended vehicle or a house left unattended for longer than 48 hours, I will be responsible for its replacement.
- 3 I agree to: treat the laptop/tablet with due care and keep the laptop/tablet in good condition, ensure that it is strapped in to the carry case when transported and/or not in use, not leave the laptop/tablet unattended in class without being secured and avoid food and drink near the keyboard/touch pad/tablet.
- 4 I agree to back up my work on a regular basis. I understand the WSAPC will not accept responsibility for the loss of work in the event of the laptop/tablet malfunctioning.
- 5 I agree to only use software licensed by the college, authorised by the Co-Head Teachers and installed by the ICT Development Manager or delegated employee.
- 6 I agree that Anti-Virus software is installed and must be updated on a weekly basis. The ICT Development Manager will advise on the routines and schedule of this operation.
- 7 Should any faults occur, I agree to notify the ICT Development Manager as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or anyone other than ICT Development Manager or the ICT technician, attempt to fix suspected hardware, or any other faults.
- 8 I agree to attend training in how to access the Curriculum Network, Intranet, VLE (Edmodo), Internet, and email within the college provided by responsible persons.
- 9 I agree that home Internet access is permitted at the discretion of the Co-Head Teacher. I understand the WSAPC will not accept responsibility for offering technical support relating to home Internet connectivity.
- 10 I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than WSAPC/WSCC premises are not chargeable to the college.



11 I agree to adhere to WSAPC and WSCC policies regarding the following, updated as necessary:

- ✦ Acceptable use
- ✦ Data protection
- ✦ Computer misuse
- ✦ Health and safety

LAPTOP DETAILS	
LAPTOP/TABLE MAKE	
MODEL	
SERIAL NO.	

I have read and agree to be bound by the terms and conditions set out above

NAME	
CENTRE BASE	
DATE EQUIPMENT RECEIVED	
SIGNATURE	
DATE	

Note on Insurance

For laptops to be covered automatically under the WSAPC policies at no extra charge, they need to be included on the college's inventory. The standard All Risks insurance policy covers the laptops/tablets for theft (where there are signs of forced entry), and accidental or malicious damage. All equipment in the WSAPC is automatically covered for fire, lightning and explosion.

Laptops/tablets are not covered by the college policy:

- ✦ Whilst in vehicles
- ✦ Left unattended in a locked household over 48 hours.

Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to ICT staff. If stolen or damaged from an employee's home, WSAPC would first ask for a claim under the staff member's household policy. Claims from the WSAPC policy will only be made if this were unsuccessful.

Please note that regardless of the policy a stolen laptop/tablet is claimed under, a claim will not be considered unless there are signs of forced entry or assault.



USEFUL LINKS

Parental Controls –

<http://parentalcontrols-on.org/>

Get Safe Online –

<https://www.getsafeonline.org/protecting-yourself/>

Childnet International – Guidance for School Staff –

<http://www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation>

Parent Guides –

http://www.connectsafely.org/guides-2/?doing_wp_cron=1377162464.3179929256439208984375

CEOP (report abuse) –

<http://ceop.police.uk/>

The Internet Watch Foundation –

<https://www.iwf.org.uk/>

The Education Network

<http://www.nen.gov.uk/?s=e-safety>

Childnet International –

<http://www.childnet.com/>

Webwise -

<http://www.bbc.co.uk/webwise/0/>

Insafe -

<http://www.saferinternet.org/web/guest/activity-book>

South West Grid for Learning -

[http://www.swgfl.org.uk/Staying-Safe/Digital-Literacy-\(1\)/Download-Page](http://www.swgfl.org.uk/Staying-Safe/Digital-Literacy-(1)/Download-Page)

London Grid for Learning -

<http://www.lgfl.net/esafety/Pages/education.aspx>

Keeping Children Safe Online -

<http://www.internetmatters.org/>

DfE Guidance -

<https://www.gov.uk/government/publications/preventing-and-tackling-bullying>

Safer Internet –

<http://www.saferinternet.org.uk>

Kidsmart –

<http://www.kidsmart.org.uk>

Digizen –

<http://www.digizen.org/cyberbullying/film.aspx>

Grid Club and the Cyber Café –

<http://www.gridclub.com>

Think U Know –

<http://www.thinkuknow.co.uk>

