an RSA academy

Whitley Academy

# APPENDIX 27

## Health & Safety Policy

## INTERNET SAFETY
## & CYBER BULLYING

**Updated: April 2016**
**Approved at Resource Management Committee:** June 2016

**NEXT REVIEW Summer 2018 – (Every 2 years)**

## CONTENTS

Introduction Page 3

Aims Page 3

e-Safety – Roles and Responsibilities Page 3

e-Safety in the Curriculum Page 4

e-Safety Skills Development for staff Page 4

Managing the School e-Safety Messages Page 4

Parental Involvement Page 5

What is cyber bullying? Page 5

How cyber bullying may be carried out Page 6

Preventing cyber bullying Page 6

Practices and procedures Page 7

Responding to cyber bullying Page 7

Investigation Page 7

Working with the perpetrator Page 7

Further incidents of serious cyber bullying Page 8

Support for the person being bullied Page 8

Civil and criminal law Page 8

The role of the Governing Body Page 9

Appendix 1 – Behaviour for Learning Page10

Appendix 2 – Cyber Safety Code Page 12

Appendix 3 – Student Advice Page 13

Appendix 4 – Staff Advice Page 15

Appendix 5 – A-Z Guide: Language and Media of Cyber-Bullying Page 19

Appendix 6 - ICT Acceptable User Policy Page 24

## Introduction

Whitley Academy fully supports the importance and usefulness of modern cyber technology. There are risks involved in its use and cyber bullying and abuse of resources will not be tolerated at our school, and every effort will be made to eradicate it.

Internet safety and awareness of cyber bullying is embedded within our schemes of work, and online safety and child protection issues are raised at least once a term. We aim to educate our students to be aware of the dangers of technology and empower them to use it for the good of all and harm no one. New CEOP resources become available in February each year and we deliver a whole week of lessons and assemblies for all groups. Access to technology capable of facilitating cyber bullying is limited to networked computers, and the main areas identified as a potential tool for cyber bullying are blocked as far as possible. The school's E-Safety Officer is Mr S Steinhaus (Vice Principal) and the Child Protection Officer is
Mr P Rule.

## Aims

This policy aims to ensure that:

- Pupils, staff and parents are educated to understand how to stay safe when using digital technology, what cyber bullying is and what the consequences are.
- We have the knowledge, policies and procedures to prevent and, if necessary, deal with cyber bullying and other e-safety issues in school or within the school community.
- We monitor the effectiveness of our counter measures.

## eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety Co-ordinator in this school is
Stephen Steinhaus who has been designated this role as a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the ICT Curriculum Leader Mr Patel to keep abreast of current issues and guidance.

Senior Management and governors are updated by the ICT Curriculum Leader through the ICT Strategy Group and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

## eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT, Citizenship lessons and tutor periods
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils about the online risks that they may encounter outside school is done through assemblies, Citizenship lessons and tutor periods
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

### eSafety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

### Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the pupils at the start of each school year
- eSafety posters will be prominently displayed
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on.

### Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/Carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by publication on website and parental consultation evening
- Parents/Carers are asked to read through and sign acceptable user agreements on behalf of their child on admission to the school
- Parents/Carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (eg on school website)
- Parents/Carers are expected to sign a Home School agreement containing the following statement or similar

  → **We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community**

- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information and celebration evenings
  - Practical training sessions e.g. How to adjust the Facebook privacy settings
  - Posters
  - School website
  - Newsletter items

**<u>What is cyber bullying</u>?**

- Sending or posting harmful or upsetting text, images or other messages using the Internet, mobile phones or other communication technology.
- This can include threats, intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images.
- It can take many forms, and can go even further than face to face bullying by invading home and personal space, and can target one or more people.
- It can include messages intended as jokes, but which have a harmful or upsetting effect.
- It can take place across age groups and target pupils, staff and others.

**<u>How cyber bullying may be carried out</u>**

- Threatening or bullying e-mails possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent during instant messaging.
- Threatening or embarrassing pictures and/or video clips via mobile phone cameras.
- Threatening, intimidating or upsetting text messages.
- Silent or abusive phone calls or using the victim's phone to harass others and make them think the victim is responsible.
- Menacing or upsetting responses to someone in a chat room.
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites such as Face book.

**<u>Preventing cyber bullying</u>**

- Staff and students are encouraged to stay safe by being told the importance of password security and the need to log off from accounts.
- Internet filtering reduces the chances of cyber bullying.  Students up to Post 16 <u>do not</u> have access to social networking sites, nor are they able to access web-based e-mail.
- Pupils have access to the Internet safety and cyber bullying web sites and resources, and are aware of where to get help if they need it.
- Pupils are encouraged to talk to any member of the ICT staff if they feel they are being cyber bullied.
- Staff and pupils have to sign an acceptable user policy (Home School Agreement).
- Resources are on the network and staff, including non-tutorial staff, are expected to watch the video and read the guidance.
- Posters are in every ICT room and parents are advised regarding cyber bullying and Internet safety at Open Evenings.
- School newsletters often include articles regarding Internet safety etc.
- All students must sign the school's Acceptable User Policy (or accept when logging in at the start of the year).
- Parents are encouraged to support the online safety of their children at home and are made aware of the dangers and problems associated with unrestricted, unmonitored Internet access, whether by computer or by mobile technology.
- The Principal has appointed a member of staff (Mr S Steinhaus – Vice Principal) to act as an E-Safety Officer to oversee the practices and procedures outline in this policy and to monitor their effectiveness.
- The E-Safety Officer will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing bullying.
- Staff will be trained to identify signs of cyber bullying and will be helped to keep informed about the technologies that children commonly use.

- A code of advice (see Appendices 2 & 3) is developed, periodically reviewed and communicated to help students protect themselves from being caught up in cyber bullying and to advise them on reporting any incidents.
- Contact with the Internet Watch Foundation, the Police or the Safeguarding Children Board Officer if images might be illegal or raise child protection issues.

**Practices & Procedures**

- The school will encourage safe use of ICT, emphasising the importance of password security and the need to log out of accounts.
- CPD and INSET will be used to help staff develop their own practices and support pupils in safe and responsible use of ICT (hot spotting etc).
- Positive use of ICT will be promoted and the Acceptable User Policy will be kept under review as technologies develop.
- The school will promote the message that asking for help is the right thing to do, and how cyber bullying can be reported.
- The school will run regular E Safety parents evenings
- Confidential records will be kept of all cyber bullying incidents.
- The school will carry out an annual e-safety audit for all stakeholders.

**Responding to cyber bullying**

Any incident of cyber bullying should be handled in accordance with Whitley Academy Anti-Bullying Policy.

**Investigation**

- The student being bullied should be assured that they have done the right thing in reporting the problem and that action will be taken which does not place them at further risk of bullying of any kind.
- Student, staff and parents are advised to keep a record of the bullying as evidence, eg phone logs, images, text messages.
- Once the situation has been resolved the student (victim) will be monitored by the form tutor and Learning Support Caseworker to ensure that there have been no further incidents.
- School staff may confiscate a phone or device if they believe it is being used to contravene the School Behaviour Policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the Police for further investigation.
- Follow normal procedures and if required contact local police (Tel 101)
- All cyber bullying incidents are thoroughly investigated and recorded in the school's Bullying Log Book.
- When evidence has been secured, the offensive material should be removed or deleted from the relevant device.
- Contact the Internet Watch Foundation, the Police or the Safeguarding Children Board Officer if the images might be illegal or raise child protection issues.

**Working with the perpetrator**

- Once the student(s) responsible for the cyber bullying has been identified it is important that, as in other cases of bullying, sanctions are applied. Steps should be taken to change the attitude and behaviour of the bully and a restorative approach may be appropriate. Parents/carers of all students involved would be included and consideration would be given as to the appropriateness of involving outside agencies. Work with the perpetrator and any sanctions will be determined on an individual basis, with the intention of:-
  - Helping the person harmed to feel safe again and be assured that the bullying will stop.

- Helping perpetrators to recognise the consequences of their actions and facilitating change in their attitude and behaviour.
- Holding the perpetrator to account so they recognise the harm caused and do not repeat the behaviour.
- Demonstrating that cyber bullying, as any other forms of bullying, is unacceptable and that the school has effective ways of dealing with it, such as:-
  * Loss of social time, break/lunch time for a specified period of time.
  * Put on report to monitor behaviour towards others.
  * School detention.
  * Isolation.
  * Ban from bringing a mobile phone into school for a specified period of time.
  * Limiting of Internet access for a specified period of time.

**<u>Further incidents of serious cyber bullying</u>**

- A recommendation may be made to the Principal for a fixed-term exclusion.

**<u>Support for the person being bullied</u>**

- Emotional support and reassurance that it was right to report the incident(s).
- Advice not to retaliate or reply, but to keep the evidence and show or give it to their parents or a member of staff.
- Advice to how the perpetrator might be blocked from the individual's site or services.
- Advice to consider changing e-mail address and/or mobile phone number(s).
- Actions, where possible and appropriate to have the offending material removed.
- Discuss contacting the Police in cases of suspected illegal content (see appendices 2 & 3 of this policy for further details).

**<u>Civil & Criminal Law</u>**

Although bullying is <u>not</u> a specific criminal offence in UK law, there are laws that can apply in terms of harassing or threatening behaviour. Some cyber bullying activities could be a criminal offence under a range of different laws, such as:

- 'Protection from Harassment Act 1997' which has both criminal and civil provision.
- 'The Malicious Communication Act 1988'
- Section 127 of the Communications Act 2003'
- 'Public Order Act 1986'

**<u>The role of the Governing Body</u>**

The role of the Governing Body is to:

- Monitor the effectiveness of this policy and its regular review.
- Receive reports from the Principal or nominated person as appropriate regarding monitoring, logging and management of cyber bullying incidents.

**Appendix 1**

**Behaviour for learning – misuse and abuse of ICT facilities**

The Whitley Academy Home-School Network Agreement exists to provide clear expectations about ICT use in school. The main premise of the agreement is that pupils will use the school computers responsibly and with care.

Students must not:

- Play games i.e. activities that are solely for fun and / or not related to a curriculum aspect.
- Use emails in an inappropriate manner
- Access irrelevant, inappropriate web sites through free "surfing".
- Log on as other pupils and steal user identities

Students should leave the equipment alone and not fiddle with any aspect of the hardware or operating software.

**BFL responses**

If a pupil is caught accessing irrelevant web sites/games sites/software or using email in an inappropriate manner **or** fiddling with the hardware or operating systems i.e. opening / shutting disc trays / playing with monitor settings :

1. Immediately make it clear to the pupil that the behaviour is not part of what they have been asked to achieve and insist they exit the web site/software and return to the directed tasks.
2. If they repeat the offence issue an immediate C2 and log it on the SIMS system. Email NWi who will arrange to have the pupils access to the Internet and/or email removed for up to four weeks. The Pastoral Progress Manager will contact the Parents to inform them of this problem.
3. If a pupil is reported three times in total over a year they will have their access to the entire network removed and parents will be invited in so that the Home-School Agreement can be renewed.
4. During any time where access to the internet has been removed, pupils may have very limited access to certain sites essential to complete examination work. This will be managed through creation of a 'white list' after consulting with the appropriate teachers.

**If a pupil is caught logging on as another pupil or causes actual damage to the hardware or operating system**

1. Issue an immediate C4 and call Reception to have duty staff remove the student to isolation.
2. Complete a C4 referral in SIMS and inform NWI who will remove the pupil's network access. NWI will contact the Pastoral Progress Manager by email who will contact parents.
3. The Pastoral Progress Manager will contact parents for a meeting to discuss the incident and revisit the Agreement with them and the student.
4. A repeat of the above will result in a fixed term exclusion from school for three days in the first instance.

**Appendix 2**

## Cyber Safety Code

### Three steps to safety

1. Respect other people – online and off. Don’t spread rumours about people or share their secrets, including phone numbers or passwords.
2. If someone insults you online or by phone, stay calm. Ignore them, but tell someone you trust.
3. “Do as you would be done by!”. Think how you would feel if you were bullied. You are responsible for your behaviour – so don’t distress other people or encourage others to do so.

### If you are being bullied

It is never your fault. It can be stopped and it can usually be traced.

- Don’t ignore the bullying. Don’t reply, but do tell someone you can trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you seem frightened or angry it will only make the person bullying you more likely to continue.

### Text / Video messaging

- You can turn off incoming messages for a couple of days.
- If bullying persists you can change your number (ask your mobile phone provider).
- Do not reply to abusive or worrying messages. You can report them to your mobile phone provider.

### E-mail

- Never reply to unpleasant or unwanted messages.
- Don’t accept e-mails or open files from people you don’t know.
- Don’t delete bullying e-mails – print them or save them as evidence in a separate folder.

**Appendix 3**

## Student Advice

### Social networking sites, chat rooms and instant messaging

- Change privacy settings so you can choose who to be friends with and who can see your profile.  Don't add anyone you don't know to your friend list.
- Don't use your real name in chat rooms.
- Never give out your photo or personal details, like your address, phone number or which school you go to.
- Don't post any pictures or videos you would not be happy for your parents or teachers to see.  Once they are online they can be copied and posted in other places where you can't get rid of them.
- Keep your password private and don't tell anyone, not even your best friend.
- To report suspicious behaviour online and to learn more about keeping yourself safe online visit www.thinkyouknow.co.uk

***Always report bullying incidents.  Not doing that allows the bully to continue.  That's not good for the victims, for those who witness the incidents or for the bully, who may need help to change their antisocial behaviour.***

### Useful Contacts

### Phone helplines:

- Childline – Free 24 hour helpline for children and young people:  Tel: 0800 1111
- Get connected – Free confidential helpline for young people (open 1.00pm-11.00pm every day) Tel: 0800 8084994
- Parentline Plus – Support for parents /carers:  Tel: 0800 800 2222
- Samaritans – Helpline for those in distress: Tel: 08457 909090

### Websites

Many of the Internet service providers, mobile phone companies and social networking sites have useful advice and safety tips for users and parents on their own websites.

- Childnet – A range of resources for schools, for children and young people, for teachers and for parents (www.childnet-int.org)
- Cyberbullying – Providing advice around preventing and taking action against cyber bullying (www.cyberbullying.org)
- Chatdanger – Website that informs about the potential dangers online (including bullying) and advice on how to stay safe while chatting (www.chatdanger.com)
- Netsmartz – Online safety site with activities for children, young people, parents/carers and for professionals (www.netsmartz.org)
- Thinkuknow – UK online safety site of the Child Exploitation and Online Protection Centre with lots of information and activities (www.thinkuknow.co.uk)
- WiredSafety – An American Internet safety site with lots of information and activities (www.wiredsafety.org)

**Appendix 4**

## Staff Advice

### Health & Safety

Both pupils and staff should be trained on the safe use of ICT facilities and should be provided with appropriate information and equipment to avoid risks such as repetitive strain injury (RSI) or back problems arising from inappropriate use.

### Using facilities for professional purposes

- It would be inadvisable for teachers to access chat rooms either for professional or personal purposes without first obtaining written authorisation to do so. Social networking (ie Face Book, You Tube, MySpace, Twitter etc) is not allowed during school time. For more guidance on Face Book please follow the link below:
  http://www.hull.nasuwt.org.uk/Facebook%20Guide.pdf
- All software requires admin privileges to install – as a result the ICT technicians are able to do this. For any products required that are not available to technicians, through Whitley Academy, licences have to be authorised by SLG before they can be placed upon a user's laptop / machine. The current and only exceptions to this are iTunes for staff and Chrome for Post 16.
  As an academy we have a legal obligation to be fully licenced for the software that we use. If we don't then we are breaking the law. Where there is a business case for the software it is ordered and installed. There should be no software that teachers need to install without permission. As soon as the ICT technicians receive the software, the technicians create a new build and roll it out as soon as practically possible.
- Pornographic sites should not be accessed under any circumstances. Any teacher who uses the school Internet facilities to download pornographic material is likely to be judged as committing an act of gross misconduct. On an occasional basis, following reports from staff about students accessing inappropriate materials, the ICT technicians need to access these sites to verify and to block such sites.
- Access to other offensive or inappropriate sites should be avoided. There may be circumstances where access to such material is necessary to inform teaching and learning. In such cases, prior permission to use such material should be obtained.
- The actions of all users of the Internet can be traced. Internet users leave a record in the browser of everything they have looked at, and of all e-mails sent or received. If inappropriate material is inadvertently accessed or received by pupils or staff, this must be reported immediately to the person with overall responsibility. Browser histories can be deleted; Whitley Academy logs all web traffic for students and staff through a web filter, which users do not have access to. With regards to e-mails; the sender, recipient and subject title have to be retained; the content of the e-mail itself does not.
- Great care should be taken to ensure personal access passwords remain confidential to avoid misuse by others.
- All digital and mobile devices must be password protected.
- A common sense approach should apply to the use of the Internet by teachers for personal purposes.

### General information for staff

- If a virus scan is running, don't be tempted to switch off your computer.
- Password protect your PC.
- Do not let your family, friends or students use your PC or laptop.
- If you download free music, videos or software using U Torrent, LimeWire, Kazaa, Bearshare, Morpheus etc. you risk allowing hackers access to your computer.

- Do not listen to your family when they insist they know a download site that is ok to use; there is no such thing.

**Browser safety**

- Always check that the address bar https:// is on any page where you enter a password or credit card details, verify that the address is correct and check for the security lock symbol.
- Do not let your browser remember your password for you; type it in each time.
- Regularly clear private data from your Internet history.

**General privacy**

- The browser will record websites that you visit. The browser may offer to remember certain fields in forms. The ISP may record websites that you visit but will not record data entered onto said websites. The websites will probably record the pages that you visit at that website.
- All of this information is backed up to Internet active sites where it will be available for a considerable period of time. Face Book will store information.
- Every network aware device has a network card. For example, the wireless network card in your laptop has a MAC address and the wired network card in your laptop has a MAC address. The Bluetooth adaptor in your laptop may also have a MAC address. A MAC address is unique but it is not technically unchangeable. There are many applications available that let you temporarily make other devices on your network see your MAC address as something other than the MAC address of the Network Card.
- Your MAC address is still the same; it is just pretending to be something different.
- Webmail e-mails such as Google mail and Hotmail also have the facility to trace the source of information sent.

**Social networking sites (YouTube, Face book, MySpace, Twitter etc)**

- It is impossible to be completely private or anonymous.
- Change privacy settings to allow only friends to see your profile – by default anyone can see your information.
- Do not put anything in your profile that could be used to compromise you.
- Do not add pupils.
- Do not use your real date of birth, job title, educational history etc – these can be used by identity thieves.
- Whenever you post anything online, think about how it could be construed and whether it could cause anyone to question your motives.

**School laptop security**

- You are responsible for the data you use, store and access via your laptop, whether at school, home or in transit.
  If it is stolen the thief could potentially an access everything, including personal e-mails, online accounts, websites and all files.
- Separate personal from professional. De-personalise your school laptop. Store your data on the school network, where it is safe and backed up regularly. Only work related data should be stored on the school network.
- Laptops should be password protected and have the drive encrypted to protect data. At Whitley we have an incredibly strong password which should help prevent password loss and we have a plan in place to start encrypting laptop drives during the summer term (2013).

**Staff Acceptable User Policy**

- Students and their families sign a policy in Year 7 to say that they will follow school guidance for safe use of the school network.

- Staff also sign an AUP when logging on for the first time. (This function was removed during the 2011 migration to Windows 7 as it was incompatible. The ICT technicians will shortly be rolling out a package that will restore this function).
- Good practice includes:
  - clean desktops
  - clean files and folders
  - appropriate use of internal e-mails – do no forward spam or send scattergun e-mails

**Helpful links**

https://www.facebook.com/safety
http://www.ceop.police.uk

**APPENDIX 5**

| A-Z Guide: Language and Media of Cyber-Bullying | |
|---|---|
| **Site/Term:** | **Description/Definition:** |
| about.me: | Among the lesser known Facebook-style social-networking sites, and important for that reason. Pupils may use more obscure sites to 'hide' malicious activity, often posting URLs to peers to extend their 'fun'. |
| Adding: | To add someone online is to accept or initiate a connection with someone, usually on a social networking site. You may or may not already know them. See also Friending. |
| ask.fm: | The Latvian social-networking site at the heart of the Hannah Smith tragedy, ask.fm allows users to ask and answer each other's questions. Users may control the anonymity of their profiles, meaning that any malicious behaviour is immensely difficult to trace. Note too the difficulties of content regulations given its overseas status. |
| bebo.com: | Originally founded in 2005, Myspace competitor Bebo was eventually sold to AOL in 2008 for $850 million and has since faded into obscurity. The brand is set to be re-launched as an 'apps' publisher this year. Their flagship products include the video walkie-talkie app 'Blab', and another two releases that are yet to be named. Definitely one to be aware of for the future. |
| Blog: | Short for 'web-log', a blog is an online space where users can record their thoughts (usually in considered prose), opinions and links to other pages and sites. |
| blogspot.com: | A 'blogging' site where users can post extended thoughts, comments and analysis. You should be aware that those who suffer from bullying, as well as those who perpetrate it, may write online about the way they are feeling. |
| buzzfeed.com | This is one of the most popular producers of online news, entertainment and visual content in the world. Its features – from politics and current affairs to the more trivial quizzes and 'ten things you need to know about….' pages – frequently go viral (see 'viral' below). Users may send each other articles which, though they contain nothing personally relevant to the reader, could be used malevolently, eg 'ten reasons why you're failing at life.' |
| chatroulette.com: | As its name implies, chat roulette allows users with webcams and microphones to cycle through a selection of other online users around the world, see and speak to them both directly and via instant messaging. It is notorious for its numerous sex webcam users, and presents a real danger to young people. You should prohibit accessing it using school/college equipment, and you should warn your pupils that using it light-heartedly on any electronic device is not acceptable. |
| dropbox.com: | Dropbox is a real boon for teachers who may wish to back-up and/or share large amounts of information, larger files, images, videos or documents among their pupils. But that capability can also be used maliciously, allowing instantaneous transfer of material to potentially thousands of users. |
| facebook.com: | Arguably the biggest social-networking phenomenon in the history of the internet, Facebook is used by millions of people worldwide, and combines individual profiling with content sharing and an instant messenger service. You should beware of the use of invite-only and approval-only Facebook groups that can be used to deliberately exclude specific individuals from participating in content sharing and its instant messaging service being used to harass others. Note too the dangers of location tracking. Unless it is |

| | |
|---|---|
| | turned off, users' Facebook posts will include details of their exact geographical location, putting them at risk of contact with those who might wish to use physical intimidation instead. Ensure your internet policy specifically includes Facebook use. |
| FaceTime: | This live videophone app is only found on Apple products and is most commonly found on the iPhone. Effectively the Apple version of Skype, it offers the opportunity to intimidate vocally and visually, but also to exclude owing to its selected distribution across the Apple family only. |
| flickr.com: | Originally a photo-posting and sharing website for professional and semi-professional photographers, flickr is now emulating Facebook but with even greater emphasis on visual content. Less likely to be used by bullies, but certainly a place where malicious imagery can be hidden among millions of other photographs. |
| Friending: | The act of accepting a connection with another social networker, regardless of whether you know them or not. |
| Fraping: | Controversial because of its sexual connotations, fraping involves using – 'raping' – another user's Facebook account without their permission (though do note the term now applies to other social media, eg Twitter). This typically involves an unattended phone or computer being commandeered for the posting of embarrassing or malicious statuses on the user's behalf and without their permission. Make sure your staff and students know that this is unacceptable behaviour and that they do everything they can to protect themselves against invasions of personal internet space. Above all, never leave accounts open when you are not at the computer or phone. |
| Google+: | Google own-brand social-networking site is by no means as popular as Facebook remains, but it has several features which could post risks to your pupils. Firstly, its in-built photo editor allows users to add a variety of Instagram-like (see below) filters and more complex hues and taints. If a victim's account is hacked their pictures could potentially be deliberately tampered with using this service. Note too that Google+ also offers location tracking. |
| Gifboom: | A gif (graphic interchange format) is a visual animation made of sequenced images, and Gifboom allows you to make them using your own phone camera and add captions or text. A gif's animation speed makes for a potentially amusing format which may be used to mock or harass your pupils. Definitely a step up from the camera phone capability that allows students, for instance, to 'happy slap' their peers. |
| Grindr: | The app that inspired 'Tinder', Grindr offers the same package as Tinder but for homosexuals. It is to be noted for its highly sexual content. Allowing users to quickly flick or 'swipe' through each other's profiles and make split-second judgements about their sex appeal. Grindr is dangerous not least for its potential to put its users in written and physical contact with those they meet online. It may also be used to harass the pupils at your school, eg bullies may deliberately set up an account on behalf of someone else in an effort to 'out' them. |
| 'Happy Slapping' | A malicious phenomenon that emerged following the widespread inclusion of cameras in phones, happy slapping involves bullying someone (usually involving physical violence) and deliberately filming it. These videos may be uploaded to the internet (YouTube) and then deleted from the culprit's phone, making it a difficult thing to police and regulate. |

| | |
|---|---|
| I Can Has Cheezburger | Originally one of the biggest sites for 'memes' featuring the so-called 'lol-cat'. I Can Has Cheezburger features viral visual content of all kinds. It may be a source of animations and visual content for those who want to humiliate others, eg a student who is bullied for being mall may be sent a 'gif' of a Chihuahua as a means of emphasising their size. |
| Instagram | A photo-editing and much-criticised sharing application that allows users to add a 'professional' tint to their handiwork. Beware its location tracker and the potential for exclusion by other users, who have the choice whether or not to 'add' or 'follow' their peers or not. |
| Last.fm: | A music website that uses the music recommending system "Audioscrobbler", Last.fm builds lists of music that are tailored to the styles of music you access on the internet, your computer or any corresponding music-playing devices. You should be aware that it accesses information on your computer or corresponding devices and that its focus on 'trending' music offers ammunition for the exclusion of others. |
| LinkedIn: | A networking site and application for professionals looking to connect with colleagues old and new, or look for a new job. Perhaps not commonly found in use by younger pupils, but does give bullies real ammunition if they wish to tarnish their victim's reputation or image online. A hacked account could result in real embarrassment, especially in front of potential employers. |
| LOL: | An abbreviation of 'laugh out loud'. |
| Myspace: | Once the talk of the social-networking world, Myspace has now decreased in popularity and is not being marketed as a social-networking/personal music sharing site. Users who did not delete their accounts before switching to other sites will provide ammunition to bullies who may use older photos and posts to embarrass their victims. |
| OM(F)G or OM(FU)G: | An abbreviation of 'oh my (f*****g) God'. |
| PM: | Private, or instant, messaging, PM denotes a live messaging system internal to a social networking site, eg 'I think I left my jacket in the library yesterday, PM me if you find it tomorrow'. |
| Ratemyteachers.com: | This site provides an online space for pupils to anonymously rate their teachers. Pupils score their teachers out of 100 for easiness, helpfulness and clarity respectively and there is also a comment box. Pupils' anonymity means that it is extremely difficult to catch those who post malicious things about their teachers, and your staff may be shocked by the fact that their pupils control whether they are registered on the site or note. Definitely one to watch for pupil-teacher cyber-bullying. |
| Selfies: | Short for 'self-portrait', the selfie is typically a photograph taken on a camera or camera phone. Popularised by (often irresponsible) celebrity endorsement, selfies can be used to cyber-bully if they are used to foreground the user's indifference towards another pupil being mistreated. For instance, a pupil who takes a picture of themselves smiling while another pupil is being beaten up is behaving inappropriately. They also count as 'sexts' if taken in an illicit way. The distribution of selfie sexts without the takers' permission is likewise inappropriate and illegal. |
| Sexting: | A portmanteau of 'sex' and 'texting', sexting is the sending of sexually explicit messages and/or images, often between phones but also via instant messaging services. Their content is inappropriate in schools. They pose a risk both to pupils who may feel pressured to engage in underage sexual activity, and to those whose privacy is compromised by the malicious |

| | |
|---|---|
| | distribution of sexual imagery or writing. |
| Skype: | An online video-calling service which allows users with webcams and microphones to talk to each other for free.  Note too its instant messaging service. |
| Status: | A term born with Facebook, a status is a user’s most recent post.  It could be a thought, feeling, location, picture or video. |
| Tinder: | The heterosexual incarnation of Grindr, Tinder is dangerous not least because it has become a marketplace for sex.  Profile images are usually in some way sexualised and escort services advertise using its free profiles.  Its ‘swipe-right’ culture – whereby users can quickly flick through others’ descriptions and choose ‘matches’ – can bring strangers into written and physical contact with one another.  Its internal messaging system is likewise a potential breeding ground for malicious behaviour, and, though it does not offer the precise location of other users, it is possible to ascertain a rough estimate. |
| Trolling: | The act of deliberately annoying someone on the internet by sending or responding to internet content with provocative imagery, text or audio.  An example might be responding to another user’s Facebook post about their love for family with a ‘meme’ that uses deliberately misspelled text and a relevant image from a popular film or television show to belittle the original poster. |
| Tumblr: | An online blogging platform that allows users to share multimedia to build their own blog.  Tumblr is immensely popular and features nearly 200 million blogs.  Users can search blogs and will be presented with matches based on the hash-tagged topics they search for.  Much of its content is fun and/or meaningful, but you should be aware too of its sometimes sexualised content, and the easy access the site provides to private ‘soft porn’ imagery. |
| twitter.com: | Arguably Facebook’s biggest competitor, Twitter is a social networking programme that allows users to share and view multimedia, and post their thoughts in 140-character-or-less ‘tweets’.  ‘Tweeters’ will receive a feed of information from other users based on the people that they ‘follow’, and the opportunity here to follow celebrities is one of the brand’s unique selling points.  Twitter feuds are all too common though, as it offers users ample opportunity for communication with complete strangers from around the world. |
| Viral: | An adjective used to describe online content that has become globally popular.  Viral content would typically receive millions of views in a short space of time. |
| Whatsapp: | A multi-platform messaging and multimedia sharing app available for iPhone, Android, Blackberry, Nokia, Symbian and Windows phones, Whatsapp offers users the opportunity to message one another whilst bypassing the cost of normal texting via mobile phone networks.  It requires an internet connection, and you should be aware that pupils using it need not necessarily have access to your school‘s Wi-Fi network to use it and be online. Be aware also of the risk of exclusion bullying and/or bullying via photo sharing and sending. |
| YouTube: | Now owned by Google, YouTube is globally the most famous video-posting and sharing site.  From amateur video blogs to official film trailers and the music channels of the world-famous bands, users can access an enormous collection of visual and audio multimedia at the click of a button.  Though its sexual content is strictly regulated, its chat room-style comment forums |

| | |
|---|---|
| | under each video are certainly not and have become a breeding ground for 'trolls', racists and the politically incorrect. You should inform your pupils that they should exercise extreme caution when accessing any video and reading its corresponding comments. Users can see how many times a clip has been viewed; this may help decide the extent of a bullying case. |

**APPENDIX 6**

## WHITLEY ACADEMY

### Acceptable User Policy

If you have any **questions about the** policy, please contact the Vice Principal responsible for ICT.

The school assumes the honesty and integrity of its ICT users (students and staff). Facilities are provided in as unrestricted manner as possible to offer the best possible quality of service.

It is the users' responsibility to ensure that they comply with the policy. The latest version can be found on the school's website along with the following related policies.

Online Protection
Internet Safety / Cyber Bullying
E-Safety Advice for Parents

All new students (year 7 and new admissions) will be invited to sign an agreement to abide by the policy.

All staff and students will have to accept an electronic version of the policy when logging on to a school computer. Students' refusal to follow any of this policy when pointed out by a member of staff will be treated as any other refusal to follow an instruction, in line with the schools consequences procedures. These are clearly stated in the BFL network use document.

### General Policy

The user agrees not to:
Upload, download, post, email or otherwise transmit or store any content that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethnically or otherwise objectionable.

Impersonate any person or entity, or falsely state or misrepresent affiliation with a person or entity, including the forging of headers, or to otherwise manipulate identifiers in order to disguise the origin of any content transmitted through the School services.

Upload, download, post, email or otherwise transmit or store any content that the user does not have the right to transmit.

Upload, download, post, email or otherwise transmit or store any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party.

Upload, download, post, email or otherwise transmit or store any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes" etc. except when directly resulting from curriculum work.

Upload, download, post, email or otherwise transmit or store any material that contains software viruses or any other computer code, files or programs designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware; or telecommunications equipment.

Interfere with or disrupt the service or servers or networks connected to the service, or disobey any requirements, procedures, policies or regulations of networks connected to the service.

Collect or store personal information about others without direct reference to The Data Protection Act.

Use the School's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of a curriculum project.

Visit or use any online messaging service, "chat site", web-based email or discussion forum not supplied or authorised by the School.

Store or use any software not specifically installed on the service by an authorised person.

Visit, use, download, or store any game, either application or browser-based, without permission of the school's network manager and only for educational purposes.

The School reserves the right to refer any breach of this policy to the respective tutor / Learning Support Case Worker / Curriculum Leader and / Senior Leadership Group. This may result in the suspension of any or all parts of the services provided.

**Network Services**

This comprises of access to workstations (PC or Mac) in the various classrooms, labs or other areas for all users and for staff additional access in departmental offices and for those that work on the school administration network.

Storage of files for all users, including teachers and administrative staff is available on the main file server.

All users shall have complete access to any files they have created, except where ownership / authorship is in question. This is then referred to a member of the Senior Leadership Group.

Each user shall have a unique login ID and password. **The password must not be divulged to any other user or any third parties outside of the school**.

**Internet Services**

Each User shall have an Internet account to access the Internet via the School's Proxy Server. The Proxy Server will filter any unwarranted materials and be updated regularly to maintain this high level of filtering.

Any user repeatedly attempting to access such material will have their account locked and it will not be reopened until they have discussed the matter with a member of the Senior Leadership Group.

The School does not pre-screen content viewed by users, but relies on the filtering software. Should any site or content be discovered which does not comply to the General Policy it will be added immediately. We ask users to assist us with this by informing us of any offending material

**Mail Services**

All staff shall have an email account to enable them to send mail internally and externally; to take part in group conferences and to access online resources. It is viewable via the email client or via a web interface.

The size of each user's mailbox (mail storage area) will be decided by group and/or requirements to do work.

Mail sent and received externally shall be filtered for viruses, SPAM, language content and certain file types within attachments. If a user sends an email that is caught by the filters, the email will be quarantined and a request to the ICT manager must be made.

If a user repeatedly sends material that is caught on the filter the matter will be referred to a member of the Senior Leadership Group.

Any user who receives unsolicited email should forward it spam@whitleyacademy.com.

Likewise, if any user is found to be sending unsolicited emails, to other users within the school, or to external accounts, the matter will be referred to a member of the Senior Leadership Group.

Group conferences may be moderated by a variety of users, including Peer Moderation by students.

**Security**

Each User will be given a unique ID and password that will allow them to access their account. The same password will allow them to access their “Home Area” on one of the school’s File Servers and their Internet account. Passwords for members of staff to gain access to the School’s Management Information Systems (SIMS) can be changed by request of the SIMS manager.

The ID and password are solely the responsibility of the user and not to be shared with other users or third parties for any reason. If a user is found using the ID and password of another user their services may be suspended and immediately referred to their respective tutor/head of department and then the Deputy Head/Head.

The only programs that may be used within the School are those agreed on by the Network Manager and/or Senior Leadership Group and installed by a member of the Support Team. The introductions of programs (including any software containing viruses or used to disrupt any part of the network, or connected networks) onto the network is not tolerated and will be treated as intentional damage or an attempt to cause damage to School property.

All information about staff and students will be dealt with in compliance the Data Protection Act and only given to authorised agencies. Staff and students agree to abide by the Data Protection Policy.

The school reserves the right to monitor all traffic on the network, either manually or through automated software, to ensure policy compliance and to aid in resolving any issues.

By default all staff and students agree to their image or likeness to be used on the school website or in any promotional material published by the school or associated agencies unless otherwise specifically stated.

Students may not photograph, video or otherwise record other students, members of staff or members of public, whilst on school grounds, for use outside of school without explicit permission.

**Treatment of Equipment**

IT Services will endeavour to ensure all equipment is in working order. This is done by each classroom with IT equipment being checked and any damage recorded weekly, this is WA’s “MOT” system. If persistent damage occurs it will be reported to a member of the Senior Leadership Group

Should any user find that a piece of equipment does not work correctly they are to report it to a member of the support team and not attempt to repair it themselves. Members of staff who wish to receive some training in dealing with immediate repairs may make a request to the Network Manager.

Any user who causes damage intentionally or through neglect, to any equipment may be refused the right to further use of the equipment and may be asked to cover costs towards any repairs or replacements.

Unless otherwise issued to a member of staff as part of their contract (e.g. staff laptops) any equipment taken off site is the personal responsibility of the user and you are advised to check that its loss or damage is covered by your personal insurance. All such loans will require a signature by a parent, teacher and/or Curriculum Leader.

**Staff Personal Use**

The level of personal use should not be detrimental to the main purpose for which it is provided.

Personal use must not be of a commercial or profit making nature.

Personal use must not be connected with any use or application that conflicts with the staff's obligations to the school.

Staff may use email for domestic and family needs during working hours providing the level of usage does not affect their level of performance.

*Signed by Director of Finance & Operations: …………………………………..*
*(Mrs P Harrison)*
*Date: …………………*

*Signed by Chair of Governors: ………………………………………*
*(Mr T Downing)*
*Date: …………………*