# The Downley School

# Acceptable Use Policy

# October 2012

## AUPs: Context

*"Children and young people need to be empowered to keep themselves safe… children will be children – pushing boundaries and taking risks.*
*At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim."*

Dr Tanya Byron Safer children in a digital world: The report of the Byron Review

*To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."*

DfES, eStrategy 2005

## Why have an AUP?

ICT and internet access is provided to our staff and students in order to promote educational excellence by facilitating resource sharing, innovation, and communication. However, for both students and teachers, internet access at school is a privilege and not an entitlement.

Unfortunately there is the possibility that students and staff will encounter inappropriate material on the internet.

This document aims:-

- to make staff and students aware of expectations for safe ICT use
- to give staff and children the opportunity to explore new technologies in a safe way
- to show staff and children how they can report misuse

Becta (British Educational Communications and Technology Agency) stated

*"A blocking and banning approach which merely limits exposure to risk is no longer a sustainable approach. Children will experiment online, and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter."*
AUPs in context: Establishing safe and responsible online behaviours, Becta 2009

# Contents

# 1. Technologies Used

A wide range of technologies are used in school and, more importantly, at home. It should be made clear that children are not permitted into the ICT suite without adult supervision. This is made clear verbally and through signage on the ICT suite door.

The following list covers most (but not all) of the technologies we would expect the children to be using.

- The Internet
- Email
- Digital photography/video
- Webcams
- Instant messaging
- Blogs
- Podcasting
- Social networking sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with internet, camera and video functionality
- Games consoles with full internet access
- Smart phones / PDAs, with email, web functionality and cut down 'Office' applications
- Video Conferencing
- Peer to Peer networking -

Whilst staff are not expected to be able to use and fully understand all of these technologies it is expected that they are coherent regarding the risks that they pose and how both the children and themselves can stay safe if using these facilities.

Although children perhaps are not using this technology regularly it is more than likely that it will be available to them at home through parents and siblings and they need to be educated in the safe way to use it.

# 2. Internet safety and privacy

## 2.1 Using the Internet Safely

To minimise the risk of children accessing unsuitable content when using the internet, The Downley School will:

**take all reasonable precautions to ensure students only access appropriate material.**

To ensure that this happens The Downley School has accepted and uses the Buckinghamshire County Council filtering system (provided by Atomwide the county Broadband provider) which works to achieve the following:

- Access to inappropriate sites is blocked.
- Access will be allowed only to a listed range of approved sites.
- The content of web pages or web searches is dynamically filtered for unsuitable words.
- A categorising system is used to allocate web pages. Any inappropriate categories are blocked by Atomwide (see appendix 1).
- Records of banned Internet sites visited by students and teachers are logged by Atomwide.

Other benefits include:

- Accessing a site denied by the filtering system will result in a report being generated and sent to Atomwide.
- The school nominated contacts are able to immediately report the details of any inappropriate or illegal Internet material found directly to Atomwide.
- Given that the school has taken all reasonable measures to ensure that children cannot access unsuitable material, The Downley School cannot accept liability if such material is accessed nor for any consequences resulting from Internet access.

The school will immediately report any content it discovers which it believes to be illegal.

All students are taught effective online research techniques, including the use of subject catalogues and search engines. Receiving information over the web or in e-mail or text messages presupposes good information-handling skills.

Key online information-handling skills include:

- Ensuring the validity, currency and origins of the information accessed or received (for example the validity of Wikipedia);
- Using alternative sources of information for comparison purposes;
- Identifying an author's name, date of revision of the materials, and possible other links to the site;
- Respecting copyright.

The teachers and staff members will guide the childrens' research where appropriate by providing age-appropriate tools for the pupils to use.

Students will be made fully aware of the risks to which they may be exposed while on the Internet. They will be shown how to recognise and avoid the negative areas of the Internet such as pornography, violence, racism and exploitation of children. This is done through assemblies, educating parents and the School Council providing Kidsmart Training throughout the school.

If they encounter such material they will know that they should report it to an adult immediately, who will deal with it according to the school AUP.

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications. All staff will read and sign the 'Code of Conduct' and School Acceptable Use Policy before using any school ICT resources. Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability. When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

## 2.2 The Importance and the Benefit of Using the Internet

Internet use is part of the curriculum followed at The Downley School and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

The Internet allows our children access to worldwide educational resources including museums and art galleries; educational and cultural exchanges between pupils worldwide; vocational, social and leisure use in libraries, clubs and at home; access to expert advice, information and resources in many fields for pupils and staff; professional development for staff through access to national developments, educational materials and effective curriculum practice; improved access to technical support including remote management of networks and automatic system updates; access to learning wherever and whenever convenient.

The school's Internet access will be designed to enhance and extend education and it will be made clear to pupils what use is acceptable and what is not and given clear objectives for Internet use. Whilst doing this the school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law by educating staff on current laws surrounding thinks such as YouTube videos

## 2.3 Using E-mail Safely

All children have access to a Buckinghamshire Grid for Learning (Bucksgfl) email and a Downley School email, however this is not widely used. Children are encouraged to use the Downley email so that staff email addresses are protected. Students may only use their approved e-mail account/s on the school network during school time. To use e-mail safely children and staff will:

- not reveal their own or other people's personal details, such as addresses or telephone numbers or arrange to meet someone outside school via the school network. This includes usernames and passwords.
- Not reveal personal details of themselves or arrange to meet anyone without specific permission from an adult (for pupils only).
- immediately report any offensive e-mails (including chain e-mails) that they receive to an adult member of staff who will pass on the information to the headteacher. The matter will be investigated and dealt with accordingly by the headteacher (see Infringements and Sanctions for further details).
- have external, Web-based, personal e-mail accounts denied for network security reasons.
- read their e-mails regularly and remove superfluous e-mails from the server.
- not use their school e-mail address for personal reasons (e.g. online shopping, signing up for forums/chatrooms/e-mail subscription).
- only use official school provided accounts to communicate with pupils and parents/carers. Use in these circumstances should be approved by the Senior Leadership Team. It is always preferable to ask the school office to forward any email to a parent.
- ensure that any email to an external organisation is worded as carefully and professionally as any other communication that is sent on headed paper.

## 2.4 The School Website

School staff have responsibility for placing pages and information on the school website and to ensure that the content on the site is accurate and appropriate. Text written by pupils will be reviewed before publishing it on the school website and will be checked to ensure 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. The website will comply with the Education Authority's guidelines.

The copyright of all material produced by the school for display on the school's web pages belongs to the school. Permission to reproduce any other material will be sought and obtained, from the copyright owner.

The contact details for the school will include only the school's postal address, e-mail address and telephone number and a general contact No information about staffs' home addresses or the like will be published. No information regarding any of the children will be published.

The school operates an opt-out system for material and photographs of the children which are placed on the website. Parents have the option for their children's work and photograph not to be published in non-school publications (e.g The Bucks Free Press) and also for images and work not to be published on the school website or around the school.
Website photographs that include students will be carefully selected and no surnames will be published with the photographs - group photographs or 'over the shoulder' images are preferred.

## 2.5 Virtual Learning Environments (V.L.E.)

The Downley School operates a V.L.E. which is known to the pupils as TIDDLE (The Interactive Dynamic Downley Learning Environment). This may be used for a variety of activities, both academic and social. There are opportunities for children to complete work via TIDDLE and also to access a range of resources that teachers may add to their individual class pages.

Access is only granted via individual log-ins made known only to school pupils. Children have unique log-ins and passwords as set by BucksGFL. E-safety and the importance of keeping the details safe is explained clearly to the children before passwords and usernames are issued. Children are also reminded about cyberbullying and how they must not post or send inappropriate material on the V.L.E.

Courses which hold data such as children's work are password protected and require an enrolment key to gain access, something that they are only able to get from their individual class teacher. The only course that will allow guest access is the parents area, and privileges are restricted to viewing documents only. The staffroom section is hidden from the childrens' log-ins and is only visible to people with staff log-ins. All staff have teacher privileges on this course and can add and remove resources.

Each individual teacher will be responsible for the content and activities that are placed on their classes page. They will moderate any forums or chatrooms that may be live and will deal with complaints that are made as a result of inappropriate use. Whole school sections of TIDDLE will be moderated by the ICT Leader. The children have the opportunity to report any misuse in the whole school section via a forum. Any post in this forum triggers an e-mail to the ICT Leader who will deal with any complaints made to this section. Teachers may choose to omit activities from their page if they do not wish the children to have access to them.

Staff will be trained in how to moderate their pages and how they can check the activity logs of the children. Evidence is kept online of **all** activity on TIDDLE so any complaint can be supported by evidence.

Children and staff may communicate by private messages as the content of these messages can be found and checked by administrators. Current staff members with administrator privileges are listed in appendix 4.

These people have full access to all areas of TIDDLE and can alter any aspect of any course. Other teachers are given teacher privileges in their individual class course and only have privileges to alter things within it.

## 2.6 Bucks Learning Portal

Presently Governors are members of the school community with access to the Bucks Learning Portal. This is a secure area that is password protected. Currently this is used for storing meeting documents, and sharing them prior to committee and full governing body meetings. The use of this space is monitored by the ICT Leader . Usernames and passwords are generated and follow the @bucksgfl domain, in parallel with the staff accounts used

elsewhere. Governors should follow all guidelines with regards to sharing information as outlined elsewhere in this document.

As soon as a governor leaves The Downley School they will have their access privileges revoked.

## 2.7 Parentmail

The school uses an e-mail distribution list to send messages to parents, governors and staff for home school communication. All emails to home are sent via Parentmail which requires a secure log-in to access. As far as possible Parentmail will be used for mass communication to parents (for example information letters). Where parents are unable to access Parentmail a paper copy of the letter will be sent home with the child. For short notice messages (such as school closure or cancellation of extra-curricula activities) the school operates a SMS service to parents. There is a phone service for parents who are not registered for ParentMail.

## 2.8 Other communication technologies

Other communication technologies such as blogging, social network and chat rooms (e.g. Facebook, MySpace, MSN Messenger) are blocked by the school filter system (with the exception of those allowed on TIDDLE). Children will be taught the dangers of these websites in school time and also how to protect themselves by not revealing personal information. Children are free to access these sites at home with adult permission, but are reminded that sites like Facebook do require the user to declare they are over 13.

Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private. All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

Staff personal use of social networking, social media and personal publishing sites should remain professional at all times and refrain from commenting on the school, staff pupils or parents.

Mobile phones are prohibited in school for children unless there is a specific reason. Students are not allowed to use mobile devices during lessons or formal school time. It is forbidden to send abusive or otherwise inappropriate text messages using the facilities provided by the school network. If a mobile phone is brought into school it should be kept by the class teacher (in a locked cupboard) until the end of the day. Children are again reminded that they should not reveal personal information or use these technologies to threaten or abuse other children. Staff are also reminded that their personal phones should also remained locked away.

Should children feel that they are victims of cyber-bullying through these mediums then they are encouraged to report it to their class teacher or any adult in the school who will deal with the situation. If necessary the matter can be passed on the ICT Leader or a member of the Senior Leadership Team and parents will be contacted.

## 2.9 Emerging Technologies

Any emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

## 2.10 Protecting staff, child and parent privacy

The Downley School will take all reasonable measure to protect the identity and safety of all staff, children and parents.

- With regard to published children's names and photographs parental permission is requested upon entry to the school. The consent for this allows for both internal and external publication of work and images.
- No staff email address will be made public to parents or children. If children wish to contact a teacher electronically this can be done via TIDDLE.
- Parents email address will not be passed onto third parties unless permission is specifically given. Currently the only third party that holds this information is ParentMail. These are held on a secure database and permission has been given.
- No staff will associate with pupils on social networking, chat or blogging sites. No staff member will associate with ex-pupils under the age of 18. It is preferable that staff do not communicate with parents either.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## 2.11 Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. All incidents of cyberbullying reported to the school will be recorded and any incidents of cyberbullying will be investigated in the same way as any other form of bullying. The following additional steps will also be taken:

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions will applied as outlined in section 6
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

# 3. Using digital images and video safely

## 3.1 Use of still and moving images

Care will be taken when using photographs or video footage of pupils on the school website or in classrooms. Where possible group photographs rather than photos of individual children will be used and full names will not be published to reduce the risk of inappropriate, unsolicited attention from people outside the school. All images will be chosen carefully by staff members to ensure the minimum risk of misuse

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, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken.

Parental permission is obtained before publishing any photographs, video footage etc of pupils on the school website or in a DVD. This ensures that parents are aware of the way the image of their child is representing the school (see appendices for example). All children whose permission the school has not obtained are recorded in each register contained near the main office.

The school will do all it can to ensure that it is not infringing copyright or intellectual property rights through any content published on the website.

If the school website is using a webcam then this will be checked and monitored by the ICT leader to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, care will be 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, e.g. a recent case of a posting on YouTube. As a result of this mobile phones and digital cameras are banned from school.

Staff are advised not to use their personal phone or camera without permission (e.g. for a school trip). If personal equipment is being used it should be registered with the school and with a clear understanding that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

## 3.2 Technical Details:

Digital images / video of pupils need to be stored securely on the school network and old images archived after a reasonable period, or when the pupil has left the school. Individual teachers will be responsible for ensuring that these images have been deleted. However, areas of the network will be periodically checked by the ICT leader to check this has been done.

Staff will bear in mind that any image or movie file is appropriately named. Do not use pupils' names 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)

Many lessons are now using video as part of their curriculum work. Staff should not show or 'rip' any parts of films without gaining the correct copyright first (see appendices). This includes videos taken from Youtube or any other video sharing site without referencing the appropriate copyright information. This also applies to images taken from sites such as Google images, Picsearch or individual websites.

# 4. Use of the school network, data and equipment

## 4.1 General Guidance

The computer system/network is owned by the school 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 school 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.

## 4.2 Procedure for ensuring safe use

To ensure the network is used safely the school:

- ensures staff read and sign that they have understood the school's NetSmart document. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- provides pupils with an individual network log-in username. Currently Foundation Stage, and years 1 - 4 are using personal passwords. This is filtering up through the school with each academic year.
- makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have less security restrictions and inappropriate use could damage files or the network;
- 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;
- has set-up the 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;
- requires all users to always log off when they have finished working or are leaving the computer unattended;
- requires staff and pupils to always log-off and then log-on again as themselves when they find a logged-on machine (Users needing access to secure data are timed out

after 5 mins and have to re-enter their username and password to re-enter the network);

- 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.
- Has set-up the network so that pupils cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- 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;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
- Maintains equipment to ensure Health and Safety is followed;
- 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 (e.g. SENCO/Headteacher/Office admin);
- 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 (e.g. technical support from designated supplier);
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their BucksGFL username and password
- Uses the DFE secure s2s website for all CTF files sent to other schools;

- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security by attempting to access sites and machines with incorrect passwords or third party equipment.
- May search, periodically, staff areas on the school network and memory drives used by staff for inappropriate content. This will be done by the ICT leader and one other member of the Senior Leadership Team
- Virus protection is updated regularly
- Ensures that staff do not use unapproved software on work machines

# 5. Reporting Misuse

As outlined in section 2.5 children have the opportunity to report on misuse in an electronic format via a specific area on TIDDLE. This area is available to any person who is able to access the TIDDLE site with their username and password. No enrolment key is necessary. From here children are able to leave a forum post or send a personal message to the ICT Leader who will deal with the situation. Any time a post is left in the misuse forum an email alert is automatically sent to the ICT Leader so the matter can be dealt with swiftly. Children are able to remain anonymous by sending a personal message.

If a child reports misuse via email to any other member of staff then the emails should be kept and forwarded to the ICT Leader. Any documents that contain misuse should be saved and passed on to the ICT Leader.

If children are aware of anyone misusing the computer or network during school time then they can report the incident to the class teacher at the time. If the class teacher feels the issue needs to be taken further then they can report the incident to the ICT Leader. If the teacher feels it appropriate then children may be sent to the ICT Leader. Any misuse of websites should be logged with the ICT Leader who will check to see if they need to be filtered.

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 NetSmart document.

All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc). The ICT Leader will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas e.g. Bullying or Child protection log and the Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate and will inform parents/carers of any incidents of

concerns as and when required. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding in Education Team and escalate the concern to the Police if appropriate. If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.

# 6. Infringements and Sanctions

Whenever a student or staff member infringes the AUP, the final decision on the level of sanction will be at the discretion of the headteacher.

## 6.1 Students

### 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
- Misuse of personal data such as passwords and private information (one off)

*Possible Sanctions: referred to class teacher and ICT leader.*

### 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
- Persistent misuse of personal data such as passwords and private information

*Possible Sanctions: referred to Class teacher and ICT Leader, removal of Internet and/or Learning Platform access rights for a period, Headteacher informed.*

## 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, ICT Leader and Headteacher, removal of Internet and/or Learning Platform access rights for a period.*

If inappropriate web material is accessed Atomwide will be contacted so they can filter the material if necessary.

## 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 school name into disrepute

*Possible Sanctions – Referred to Head Teacher and contact with parents, removal of Internet and/or Learning Platform access rights for a period.*

Any evidence will be secured and preserved.

**In all cases parents/carers will be contacted.**

## 6.2 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.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

*Sanction – ICT Leader and Headteacher informed.*

### Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council 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 school name into disrepute.

*Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures.*

**Other safeguarding actions:**

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they will 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 Pornography being found, the member of staff will be **immediately suspended** and the Police will be called: see the free phone number **0808 100 00 40** at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

These procedures will be fully explained and included within the school's AUP. All staff will be required to sign the school's NetSmart document and have read the AUP.

See appendices for the NetSmart documents.

# 7. Complaints

Any complaints concerning a staff member, pupil or parent will be pursued following the schools established complaints procedure. The following steps will also we taken where appropriate:

- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police and/or Children's Safeguarding in Education Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions outlined in section 6) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

## 8. Communication with Pupils and Parents

All users will be informed that network and Internet use will be monitored and an e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils. It is vital that pupil instruction regarding responsible and safe use precedes Internet access.

An e–Safety module will be included in the PSHE and/or ICT programmes covering both safe school and home use. E-Safety rules will also be posted in all rooms with Internet access and safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Safe: www.safesocialnetworking.org

The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school. Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.

# 9. ICT in other policies

Cross curricular links regarding ICT and other subjects will be made clear in those documents. This section focuses and includes the wording from the antibullying and child protection policies.

## 9.1 ICT and anti-bullying

Bullying can be done through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites.

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

1. Advise the child not to respond to the message
2. Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
3. Secure and preserve any evidence
4. Inform the sender's e-mail service provider
5. Notify parents of the children involved
6. Consider delivering a parent workshop for the school community
7. Consider informing the police depending on the severity or repetitious nature of offence
8. Inform the LA e-safety officer

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

1. Inform and request the comments be removed if the site is administered externally
2. Secure and preserve any evidence
3. Send all the evidence to CEOP at http://www.ceop.police.uk/safety-centre/
4. Endeavour to trace the origin and inform police as appropriate
5. Inform LA e-safety officer

Children 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.

## 9.2 ICT and child protection

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

1. Report to and discuss with the named child protection officer in school and contact parents
2. Advise the child on how to terminate the communication and save all evidence
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services
5. Inform LA e-safety officer

# 10. Appendices

# Appendix 4

## Designated People

| | | |
|---|---|---|
| ICT Leader | - | Mr. Alastair Haywood |
| Atomwide Nominated Contacts | - | Chris Wood |
| | - | Connie Malmstrom Anderson |
| | - | Sue Webb |
| VLE Administrators | - | Alastair Haywood |
| | - | Chris Wood |
| | - | Sam Bone |
| | - | Amy Gray |