Ark Helenswood Academy

Ark Helenswood Academy

ICT & E-Safety Policy

Reviewed January 2017

Contents

1. Introduction

E-Safety comprises of the safe use of ICT including the Internet, computer hardware, electronic data and email. The purpose of this policy is to put in place a reasonable and understandable set of guidelines to ensure that we are following both a safe and consistent approach to the use of ICT within the Academy. This policy also touches upon the issues of bullying and child protection within ICT.

This document applies to every member of staff within the Academy. Teaching staff have a vital role to play within class both in educating students in e-safety, but also in following these practices when using electronic teaching materials. Associate staff have the responsibility of the safe handling and storage of sensitive data. All employees are issued with a login to the Ark Helenswood Academy network upon commencing their role, and with the use of computers, internet and email being such a prevalent feature of Academy life, this policy must be understood and agreed to.

This policy has been written in the Academy and is based upon East Sussex County Council e-safety policy and guidelines. The e-safety policy will be reviewed annually, although changes may be made at any point if necessary.

1.1 What does E-Safety Cover?

This document is divided into several sections. The first is Data Control and Systems, and describes the technical aspects of the Academy network, including securing sensitive data, being safe from external access threats and our defence against computer viruses.

The next section is on Teaching and Learning. This describes the safe use of computers within a classroom by both students and staff. It explains the use of the internet and our web filtering software, the use of appropriate teaching resources and importance of protecting personal user data. Also described in this section is the type of e-safety teaching that is given to students to ensure they are aware of the threats presented by the internet, the safe use of ICT both within Academy and at home. The section on Child Protection discusses the education we are providing for students to ensure they are aware of the correct method of safe computer usage.

2. Data Control and Systems

Within the Academy we have many systems in place to ensure that we provide a secure and e-safe working environment. Some of these systems run in the background and support our use of ICT whilst some of them will be familiar to staff. It is important that these processes run as they ensure the security of the sensitive data that we hold and the safety of those that use the Ark Helenswood Academy network.

2.1 The Ark Helenswood Academy Network

Almost all ICT usage within the Academy will be through the Ark Helenswood Academy network. The network spans the entirety of both sites with a link between the two. Computers are available for staff use throughout the Academy with students generally having monitored access in dedicated computer suites. Some staff members have laptops issued by the Academy for use both at Academy and home, and these can also be connected to the Helenswood Academy Network either wired (*plugged in using a cable*) or using the Academy's wireless network that covers the grounds of both sites.

The Ark Helenswood Academy Network can only be accessed by a registered user who is required to logon before having access to any of the Academy's programs or data. The programs that are then available to that user differ between the user type (*staff, student etc*). This could be for security reasons, as certain files or programs may only be intended for certain users, or possibly to enable tailored access for particular users depending on the circumstance. The Academy has complete wireless network coverage across both sites which is only for authorised users and is therefore encrypted to stop access from others. The encryption method in place is WPA2 which is a county recommended standard. The encryption codes and information are not shared with staff or other users and are held securely by the technical support team – there is also a "guest wifi" SSID – which is shared with guest users to the Academy. The password on this network is changed several times a year to prevent misuse – this particular wireless network also operates with a transparent proxy, so requires authentication via a Smoothwall appliance upon opening a browser before internet access is granted.

2.2 New Staff Users Network Membership

Each member of staff is issued a username and password on joining the Academy and accepting the staff code of conduct. This allows them access to the Ark Helenswood Academy computer network. Only users issued with a username and password are able to access the network. This allows use of the following:

- Staff Intranet/Internet Access
- Academy Email Account
- Shared Network Folders
- Personal 'Home' Folder

Each of these resources is available for staff use only and their content is strictly private. Passwords must be kept secure and must not be shared with other members of staff or any other users. Ark Helenswood Academy employs a strong password policy meaning that staff must have at least one

capital letter and number within their password and this must be a minimum of eight characters in length. Users are required to change their passwords every ninety days – with the policy remembering the last 7 used ensuring completely different passwords are used. The password policy also locks an account if an invalid password is entered 3 times in succession. Forgotten passwords can be reset by technical staff.

Email accounts and Personal 'Home' folders are private and can only be accessed by the individual user. However, technical staff are able to access these areas if the necessity arises. Home folders are for Academy use only and should not be used for the storage of personal files such as personal music or movies.

Staff members are responsible for their individual accounts and any attached privileges. They are held responsible for any machine that they are currently logged onto and the usage of that machine. This means that the staff member is responsible for the internet usage, modification of files, playing of content and securing of sensitive data. Staff should not leave any workstation unattended whilst logged in. Any activity on a machine is the responsibility of the member of staff. To prevent misuse the machine must be locked, logged off or shut down when unattended.

2.3 New Student Users Network Membership

Similar to staff, all new students are issued with a unique user username and password which grants them access to the Ark Helenswood Academy network. Students have slightly different access to staff with greater restrictions on the programs and folders available to them. Students also differ from staff as they are not issued an email address unless a member of the Head Girl team, or by request. Students are allowed the following:

- Student Intranet/Internet Access
- Shared Network Folders
- Personal 'Home' Folder

Upon receiving their account details on admission, students are taught the importance of keeping their password information secret. Students have private access to their home folders which can be used for storage of work and it is therefore important that other students cannot gain access to this area. Password policy is the same for students as staff, requiring a strong password and a change of password every ninety days.

Students are taught that they are responsible for their own accounts. They are responsible for any machine that they are currently logged into and the usage of that machine. Any internet usage, modification of files (*where possible*) or playing of content is the responsibility of the student logged

in. Students are also taught the importance of logging off or shutting down their machine when leaving it unattended.

2.4 Shared Network Folders

Both staff and students have access to shared network folders, although students have fewer and less access. As a result it is vital that the content stored in these network folders is suitable for public viewing. When saving a file it is important to consider who the content is suitable for and then deciding on a suitable storage location. Some drives have both staff and student access, so only student acceptable content can be stored in these locations. They are ideally for resources designed to be opened or looked at by students in lessons. Students don't have general access to save or modify files on shared network locations. There are, however, some exceptions to this where staff have arranged specific folders for students to save to (*e.g. for submitting work*).

Staff should also attempt to remove their old materials when no longer needed to avoid unnecessary space being used. Any staff member requiring more information on the correct locations for file storage should contact a member of the ICT Technical department.

2.5 Bromcom (Academy's Management Information Systems)

Most staff members are given access to Bromcom upon starting at Helenswood. Bromcom is used to store all student and staff personal data, timetable information and attendance data. Also recorded is any student SEN and personal data. This data is extremely sensitive so must be handled very carefully and in-line with Data Protection Guidelines.

Depending on the user, different access levels are available. Different content and more sensitive data may be available to a user with a higher access level. Access levels are set appropriately for the user's role when commencing, and is adjusted if necessary should that role alter at any point. The data available to users is only what is necessary for them to fulfil their role, with any unnecessary or sensitive data 'inaccessible'. Bromcom also has its own security checks, with each user issued their unique username and password when starting at the Academy.

The data stored within Bromcom is some of the most sensitive held within the Academy, so it is of upmost importance that this data is used responsibly and securely.

2.6 Printing Documents

From time to time it will be necessary for staff to print documents from their computer. When doing so make sure that you consider what you are printing and particularly where the item is going to be printing. Many classrooms don't have their own printers so instead print using a shared network

printer. These printers are often in locations where students also print, for example in the Libraries. Access to your printing job is through a fingerprint scanner and only your job can be accessed. This prevents unauthorised access to sensitive information.

When using computers in areas which do have their own printers, be sure to check the printer located nearby is actually the one you are printing to. Occasionally it is possible that another printer will become the default, even if not the logical choice, so it is necessary to ensure that you are not accidentally printing to the wrong location.

Ideally, sensitive data should only be printed when you are in close proximity to the printer so you can be certain that you will be the first to retrieve it. The above practice not only helps data control, but also reduces confusion and wastage of paper and print toner.

To avoid potential data leakage, it should not be common practice to need to print sensitive documents, this should only be done when completely necessary.

2.7 Email

All staff have access to email and are issued a unique email account. This is the preferred method of communication within the Academy, and is used to communicate important information between staff members. Like all aspects of the Academy network it is essential that any users email access is only used by that user to avoid sensitive information being shared with other parties. All users must attempt to view their emails at least once a day and preferably more frequently, as it is often a vital way of being up to date with in Academy news and updates.

- When using email there are several important points to consider, particularly when sending emails.
- Always ensure you have typed the recipient name correctly, particularly if only using initials. It is quite possible to send an email to the wrong user if you have not checked properly.
- If sending to a group always ensure you are certain of the recipients within that group and that the email being sent is suitable for all members. This is particularly important when sending to all staff.
- When attaching a file, be certain that the file being attached is the correct one, as mistakes occur if not checked properly.
- When forwarding a message ensure that any previous communications in the original message body are suitable for the new recipient. Emails are often forwarded as the latest reply is relevant, but it is necessary to check previous comments in the communication.

Staff are also urged to be vigilant of the data that they are sending to one another, especially if its contents are sensitive. Users should not pass on chain emails, and should be careful when downloading files from emails, particularly if they are from an unknown source. Any user with suspicious emails should contact the ICT Technical department for clarification first. Emails should not contain any abusive, pornographic or discriminatory content. All emails sent can be vetted should it be necessary to do so. Email should be used for work use only, and should only be used for personal circumstances if no other alternative is available.

External Staff email access is available to view emails from home. The same above rules apply, but when at home staff should be increasingly careful when viewing sensitive data. As home computers cannot be trusted as secure, no data which could be deemed sensitive should be stored on a local machine.

2.8 Intranet/Briefing

There are two versions of the Academy Intranet, a student and a staff version, both of which run in a very similar way. When loading the Internet, the first page that is displayed is the Intranet briefing page. This is effectively an online ‘notice board’ for staff members to post announcements. These can then be viewed by all other members. It is also possible to post documents and advanced features such as surveys or forums although these features are only available to the ICT technical department.

When posting a message onto the staff Intranet briefing page it is important to bear in mind that it is viewable by all staff members. It is vital that only suitable messages are posted as it is an extremely accessible location. Any messages posted should also be as informative as possible, with dates, names and rooms used (not just saying 'tomorrow' which is vague if the same message appears for a week). It is also important to bear in mind the space used by messages, and if necessary put additional information in the message body so it can be viewed if needed.

The student Intranet works in a similar manner, although the students themselves are not able to leave posts. Staff can post messages for students to read however. Again, it is important to ensure that the message is suitable for all students if posting, as the same page appears for all years and groups.

2.9 Helenswood Learning Platform

The learning platform is an online resource for use by both teachers and students. The learning platform is available both inside and outside of Academy with some areas available to the public with the rest requiring a secure login.

Every member of staff has a unique login, as do students, and this allows them each to access and create their own content. As a result, this means that any staff member could upload or create their own content, so it is important that this process is understood and managed accordingly to ensure that it remains suitable.

Please note that only suitable content should be uploaded. Content should be carefully checked for language and should not include content that could be deemed as inappropriate, especially if the content has been obtained from another source and not produced personally. Any files that are uploaded should be checked prior to uploading if only to ensure the file is the one that was intended.

It is also worth bearing in mind that whilst students have to sign in to access content uploaded for them, this cannot be assumed to be secure. It is quite possible that a student could give away their login credentials to someone else and that user could then gain access to something unsuitable for them. It is recommended therefore that anything made available to a student should also be considered to potentially be publically available.

As mentioned earlier, some initial elements of the learning platform are actually available to the public but these can only be maintained by technical staff and will only contain basic level information. The updating of these sections follows the same procedure as the Academy website, with full details available below.

2.10 Academy Website

The Academy website is an external tool for communication with parents and other interested parties. It is used to advertise events and talk about Academy success. It also holds Academy documents such as letters and results which are accessible to parents/carers of students.

As the website is public facing this means that it can be accessed by anyone, anywhere. For this reason it is very important that only appropriate data is shared and that certain important precautions are taken when choosing data to be uploaded.

All documents must first be thoroughly checked for suitability and accuracy by the person submitting the document (*this could be almost any member of staff as all departments have an area on the website*). These documents are then put into web form (*either as part of a web page or as a downloadable file*) where they are again verified for suitability and proof read by the website coordinator. Any problems are fed back to the source of the document where details are either clarified or corrected. These documents are then uploaded, at which point they are live to the public.

The other important consideration is the safety of students within the Academy. Unfortunately due to the public nature of the website there are several threats that accompany this such as potential for abduction or contact from estranged relatives. It is therefore vital that certain important steps are taken to minimise any chance of problems occurring. Where a student appears in a picture on the website they should never be named directly to maintain a level of anonymity for that student. In the same way there are some students within the Academy that, due to special circumstances, cannot be pictured for personal safety reasons. Equally any parent has the right to have their daughter not pictured on the website. Personal information on students is kept to a minimum and every effort is made to ensure that students are as anonymous as possible.

2.11 Internet Filtering

All computers connected to the Ark Helenswood Academy Network have access to the internet. This is an important and useful resource and can prove invaluable for teaching and learning. Many fantastic teaching resources are now available online, and the internet is also a great place for student research and revision.

Whilst the internet has many good features, there has to be an element of control to avoid inappropriate content being accessible. With such a wide range of pages available this is a difficult task, so software is in place to filter content as it is loaded. If content is found to be inappropriate, it is blocked preventing the user from viewing it.

The software works in several different ways. Firstly, there is a list feature which allows specified websites to be blocked. For example, if a site was deemed inappropriate the address could be added to the block list meaning it would no longer be accessible to users. Groups can be set up to enable certain sites to be available for certain users (*as an example, staff have access to more sites than students*) or even for specific times.

The most important feature of the software is its intelligent filtering system. When a page is loaded it is initially scanned by the filtering software. The software searches for 'Key' words in the document. An example might be the words; drugs, sex, games, gambling. These are all classed as 'bad' words so would have a score attached to them. Scores can differ between words, so worse words will have a higher score. To balance this there are also some words which are classed as 'good'. These words have a negative score. When a page is scanned this overall score is calculated adding all of the bad words together and then subtracting any good words. If this score is over a defined limit then the page is deemed inappropriate and is then blocked.

This provides an effective means of stopping inappropriate content from being accessed and it works extremely well. There are occasions when it actually goes too far, blocking sites which are not

inappropriate, perhaps due to the site contents (*for example sites used in PSHE*), but specific sites can be unblocked in the same way that certain sites can be specifically blocked.

Another useful feature of the filtering software is that it includes its own antivirus software. This means that it should detect viruses before they are even downloaded by the user, providing with another level of security against viruses and malware. Whilst this is not as advanced as our installed antivirus software, it is a welcome extra level of protection.

2.12 Anti-Virus and System Updates

As in all IT based environments the Academy has to be aware and prepared for potential virus attacks. Viruses can quite easily cause a large amount of damage to an unprotected network so it is important to make sure that the necessary precautions are taken.

Sophos Anti-Virus is installed on every machine within the Academy and is set to scan all new files as they are introduced to the network. This software is always running in the background and is set to automatically immunize any threats that it may come across. Full system scans can also be run upon request to ensure that a whole system is free from viruses.

Sophos Anti-Virus is set to search for new updates on a daily basis and receives these when they are available.

This means that the network is also protected against the very latest threats and ready to deal with them should one find its way onto a computer on the network.

In addition to Sophos Anti-Virus, we also have virus scanning software within our filtering software which runs initial scans on websites before data is downloaded to the user's computer. The filtering software itself will also block any pages that it suspects are supporting viruses or other malware.

Microsoft Windows updates are generally automated and sent out at suitable points by our own Windows Update Server. This allows machines to be protected against security breaches as well as being up to date with the latest software patches for improved performance. From time to time these updates need to be manually run depending on the type of update.

Other software updates are run when required to ensure that software versions are in line with the current standards. This includes software such as Flash player and Java.

2.13 Backup Processes

As a part of the Data Protection Act we are responsible for the safe storage of the data that we hold and as such are required to have a comprehensive disaster recovery plan in place. The most vital

aspect of the Academy network is the data that it holds which in many cases would prove irreplaceable.

To ensure that we have a detailed backup process in place meaning that we always have at least one copy of our data stored elsewhere. This means that if the data on the primary source is lost then it should be possible to restore from a secondary source (*and even tertiary in some cases*).

We have different procedures in place that cover us in different ways.

The first is our hard drive configuration whereby we use a type of RAID hard drive configuration which is used on many of our servers, meaning drives can easily be swapped without loss of data.

Secondly our SANs (*Storage Area Network servers*) which are responsible for storing all of our user's home directories (*students and staff*) and Academy resources (*library/staff only/administrative data etc*) are backed up at various different times of each day (sometimes up to 3 times in a single day for certain data/locations) on a disk-to-disk basis, over to the opposite site – so data stored at the upper site, is backed up to the lower site and vice versa. This off-site backup system ensures data is retrievable even after a site-wide catastrophe. Retention in some cases is up to 6 months, but as rule of thumb is kept for a minimum of 30 days.

Other backup procedures are in place and occasionally extra backups are taken, for example prior to upgrades. Restoring backed up data differs between the three options, but all are quite straight forward and quick.

Staff are responsible for the backing up of their individual data (*although files stored in their home folders are backed up as described above*) and making sure that a copy is available should the original be lost or damaged. This is important when considering many staff carry files on memory sticks which can easily be damaged, so it is vital to have a copy in another location, even if it is slightly out of date. The ideal method would be to store these files in their home folder so they become a part of the Academy backup process, but they could alternatively be stored on a staff laptop or removable media such as a CD or external hard drive.

2.14 Network Equipment and Servers

As the heart of the Ark Helenswood Academy network, the many servers provide the storage and settings for the entire network. This equipment is extremely valuable both in monetary cost and also in importance. As a result it is important that these machines are held securely and in a safe environment.

Only technical staff have access to the network servers and as such only they hold the suitable passwords to access the server software and settings. This is to prevent unauthorised access by students and staff to potentially sensitive material and to ensure that systems are kept in proper working order. Servers are kept in locked secure locations and these areas should not be accessible to students. Servers are kept in suitably air-conditioned environments to ensure that they continue to run without interruption. This also includes the use of UPS (*uninterrupted power supply*) which keep servers on should the power be lost for up to an hour, this also allows the servers to be safely shut down if mains power continues to fail.

Throughout the Academy other network equipment is located in cabinets. These are generally in cupboards and out of the way, so should not be in locations where students can access them. These cabinets do not hold sensitive data, so do not provide a security issue, but tampering with them could cause network disruption for any attached areas.

2.15 Disposal of Old Equipment

From time to time old equipment is removed and disposed of when it is no longer useful. With the expanding requirements for faster machines and more complex software, the average machine has a life of around 5 years at the end of which it is due for replacement. Other equipment follows a similar process.

When old electrical equipment is disposed of it has to be done in the correct manner following the government WEEE legislation. The WEEE directive is a government scheme which aims to improve the level of recycling of old electrical equipment, and ensure that it is disposed of in a safe and effective manner. An appropriate WEEE skip is ordered to cater for this equipment. However before any such equipment is disposed of it is first stripped of any components which may have been used to store sensitive data. Whilst it is unusual that data would actually be stored on a local drive (*this resource is generally disallowed*) is possible in certain situations that it could be possible. As a result hard drive removal is standard on all machines. Once removed, these devices are then either hardware formatted to remove data or physically destroyed. Only after these procedures can they be safely disposed of.

Any other storage media should also be disposed of in a safe manner, for example any old CDs, floppy disks or memory sticks. This could be through a thorough system format (erasing all data from the disk) or through physical destruction (*cutting a CD in half as an example*). This is a vital procedure in ensuring that sensitive data is not exposed to the public.

2.16 Copyright

Copyright covers a wide range of different areas within ICT and is difficult to cover all aspects. It is important that staff are vigilant to copyright regulations and are aware of copyrighted materials and their acceptable uses.

Examples of copyright infringement might be to duplicate copyrighted media (*for example CDs*) or to use software without the correct licence. Technical staff are responsible for the installation of software in Academy and this is carried out in line with the correct copyright and licence materials.

Full details on copyright law can be found in the legal framework section of this document.

3. Teaching and Learning

ICT is a valuable tool for both staff to use as a teaching aid, and for students for researching. However, there are pitfalls for both staff and students and it is important that we do our utmost to ensure that the use of ICT is a positive one.

3.1 Staff

With all classrooms now equipped with a computer, it is becoming second nature to involve them in teaching activities. At a minimum the computer will be used once per period for registering the class using Bromcom. Often they can be utilised as a handy teaching resource for displaying PowerPoint presentations, internet videos or smartboard interactive utilities.

Staff are increasingly reliant on data and as a result are, from time to time, in possession of sensitive data. As in all examples it is vital that this data is dealt with in the correct manner, and is held responsibly.

3.1.1 Choosing Resources

When using electronic resources with a class it is vital that they are checked carefully prior to using them. There are many useful resources which can be found, particularly online, which can enhance a lesson and are not available elsewhere. However it is extremely important to check carefully any content before using it in a live classroom environment.

Whilst filtering is in place with internet based content, it is important that any websites that are going to be used are checked thoroughly first. It is possible for a seemingly innocent looking site to contain some inappropriate content which should not be shared. Likewise, many staff are now using YouTube as a method of showing video clips in class. It is vital that these are watched in advance and in full. It is quite often found that seemingly innocent clips have been edited to have inappropriate

content added within the file. Sometimes this is as additional video footage, but often as audio recorded over the video which can often feature expletive language which would be inappropriate in a classroom environment. For this reason checking the sound on this type of content is also necessary.

It is also worth considering that not all data online is reputable so any websites required for accurate data should be checked to ensure that data is in fact correct. A good example of this is Wikipedia which, whilst a vast resource of information, is wholly user submitted, so could have mistakes or could have been purposely edited to include false information or opinion rather than fact.

3.1.2 Monitoring Computer Usage

Whilst every effort is taken to ensure that the computing facilities are tailored for proper student usage, it is unfortunately inevitable that students will find access to time wasting and inappropriate content. This will certainly be minimal due to the use of filtering software and only limited software access but it is impossible to cover all possibilities.

As in all lessons we ask that staff are vigilant of student behaviour as well as their use of computers. The best control we have over student usage is to have someone present who is aware of exactly what the students are doing.

This involves the use of the internet where staff should be aware of students browsing or any suspicious sites they might be using. Any concerns should be dealt with at the source if possible, but should a staff member see a student using inappropriate content online, he or she should report this in writing to the Head of Year and copy the report to the Designated Safeguard Lead (DSL). Logs of visited sites can be generated and unauthorised sites can then be blocked in the future. This is of course also important in making sure that students are on task and not using the internet as a time wasting tool.

Staff should also be aware of general program usage to ensure proper use of facilities but also to make sure that classroom rules are being adhered to. Students should treat the equipment with care and should not be eating or drinking in the computer suites. They should also ensure that students are not fiddling with the cabling as this can potentially cause damage to the machines and attached devices, but also carries with it a slim but possible chance of electrical injury.

Printing should also be monitored with students as this can lead to problems. Students should only print when told or if they have sought permission to do so. This prevents wasting of paper and ink, but also prevents students from printing inappropriate materials.

Teaching in an ICT classroom is not unlike teaching anywhere else, and is mostly common sense, but it is important to keep a level of awareness of exactly what your students are doing, for their benefit as well as the Academy's.

It is of course important that students are aware of the rules of the classroom when using an ICT room, and this is an important part of their e-safety training. For more details on this, read '3.2.1 Explaining E-Safety Risks'.

3.1.3 Projector Use/Displaying Content

Using the projector allows staff to display computer based resources to the class, as well as allowing for interactive smartboard utilities to be used (*in compatible areas*). This is widely used across all subject areas and is a valuable function.

It is important to remember however, that when projecting onto a board, that all computer activities are also projected for viewing. This means that if sensitive data is opened, it would be available for an entire class to read which would be unacceptable. Likewise many teachers are used to having their projector running throughout their entire lesson which could involve Bromcom being displayed for taking a register. Even this screen should not be displayed to students as it has indicators, which whilst not immediately obvious, suggest any SEN students. It is important that vigilance is paid to exactly what is being displayed on the screen when projecting.

To get round this problem there are two solutions. The first is to simply switch the projector off, especially useful if it is not going to be used for a period of time. The second, and better solution if you are planning to continue using the projector directly after displaying sensitive data, is to use the 'Freeze' feature on your remote control. This pauses the screen and any activity on the computer after this is not displayed, just the frozen image. When you want to return to the information displayed on the computer, it is simply a case of 'Unfreezing' the display using the same button.

3.1.4 Learning Platform

Staff are increasingly using the learning platform as a method for sharing resources.

It is very useful as all students can access these documents both at home and in Academy. There are a few elements that staff need to be aware of when uploading items for use.

The most important element is the data and content that is uploaded. This is discussed fully in section 2.11 'Helenswood Learning Platform'. As staff are going to be the main contributors of resources it is important that all are vigilant and aware of the necessary precautions.

3.1.5 Transfer of Data

Most staff within the Academy use memory sticks to transfer data to and from home. This allows staff to create resources and lesson plans and then bring them in from home. Some members of staff also have staff laptops which are used for a similar reason.

Unfortunately, memory sticks are small and easy to lose so present a potential data protection issue. It could be potentially dangerous for a member of staff to lose a memory stick with sensitive data stored within and for it to fall into the wrong hands. At a minimum it could create an embarrassing situation for the Academy.

As a result it has been decided that no data which could be classified as sensitive should be transferred on a memory stick. This includes data such as reports from Bromcom (*specifically those that contain students names and details*), letters containing private information, data on staff and anything else that could be harmful in the wrong environment.

This is the only option to ensure the safety of our students and staff. Alternative methods of making files accessible for home use are either to upload the documents to the Learning Platform (*and keep them private*) or even to email them to yourself (staff can send emails to their own address which can then be accessed at home). Again these practices should only be taken if it is essential, as ideally sensitive data should only be accessed within the Academy.

Laptops have their own policy which is described below, and which should be read by any members of staff who have a staff laptop.

3.1.6 External Use of Data

There should be no reason for staff users to need to take sensitive data home with them. Any tasks which might require access to sensitive materials should be carried out within Academy and not taken off of the premises. This is for reasons of data protection and is the same for electronic data as it would be to printed documents.

Any occurrences where there might be a need for sensitive data to be removed from Academy should be discussed with the e-safety co-ordinator in advance so permission can be granted.

3.1.7 Staff Laptops

The laptop Acceptable Use Policy should have been read and signed by all staff upon receiving their laptop. The main details of laptop usage are explained in that document along with all of the items also found in this document. The laptop Acceptable Use Policy can be found in section 8.2.

The most important aspect of e-safety concerning Academy laptops is the data that they could contain. As mentioned above, ideally staff should not be using sensitive data externally. However if the laptop has been used within the Academy and data loaded then it is certainly possible that the laptop could contain sensitive data.

For this reason the security of any Academy laptop is paramount and must be secured at all times. It is the responsibility of the staff member who has signed for the laptop to ensure that the data contained within is secure and that the machine is not misused in any way.

Any staff member who is concerned about sensitive data stored on their machine should contact a member of technical staff.

When a staff member with a laptop leaves their employment with the Academy, their machine is returned and all sensitive data is removed from the machine before it is reissued to another staff member.

3.2 Students

The use of ICT in the classroom is a great tool for students and it is important that students learn how to use ICT as a valuable skill. With students having such wide access to ICT both in Academy and at home, it is important that they are properly educated in its use. It is also important to make them aware of the risks involved with certain areas of computing and that they understand how best to protect themselves.

It is important that staff are aware of the provisions in place to support a safe environment for students using ICT and that they are using these correctly. An understanding of the dangers is important also in properly educating students.

3.2.2 Internet Access

As mentioned in section 2.11, the Academy has a robust Internet Filtering System installed to block inappropriate content from students. This means that students should not be able to access websites which would contain inappropriate content such as sex, drugs and violence. This also blocks time wasting sites such as games and social networking, where social networking can also present different e-safety risks.

It is important to mention that whilst the Internet Filtering System is extremely good, it is not perfect and fool proof. It is possible that inappropriate sites could be accessible through different routes with enough time spent searching for ways around. This is an unlikely scenario, but one that should be considered and protected against.

It is important that should any staff members suspect that students are attempting to bypass blocked sites that this information is passed onto the technical staff where internet usage logs can be viewed.

More information on the education of the safe use of the internet can be found in section 4. Child Exploitation and Online Protection.

3.2.3 Learning Platform

Like staff, students have the ability to upload content to the learning platform. This cannot be shared with other users (*unless specifically initiated by a member of staff*) so is for private use only.

The learning platform offers an ideal solution for students to save documents prepared at home which they need access to at Academy, and this will hopefully reduce the need for students to bring in memory sticks to use with the computers.

4. Child Exploitation and Online Protection

With children having increasing access to the internet through a range of different methods it is vital that they understand the safe use of the technology. As an emerging technology the need for this education is not unlike the same education given to children in fire prevention or road safety as it becomes a recognised part of everyday culture. It is important that this education is properly structured and refined to keep up to date with current technologies and equipment to raise awareness.

This education is not just for safe use in Academy, but also intended to help protect students in their home use. Ideally this awareness can be spread to parents and then to others to help raise general awareness.

4.1 Explaining E-Safety Risks

The bulk of e-safety training will be carried out in ICT lessons by teaching staff and will cover the whole range of e-safety issues. A unit of work on the subject is carried out each year. There will also be occasional extra sessions with students to give more detailed information on particular key areas. Some areas of e-safety will be dealt with differently as they could be upsetting and potentially difficult for some students. It is possible that some students may have experienced bullying or abuse, possibly even of a sexual nature that will be similar to the examples that will be described, some of which they may not yet have disclosed. This can cause some students distress, or even prompt them to disclose a situation as a response to the session.

As part of the curriculum in ICT, students are introduced to the ThinkUKnow training, an online training tool for students of all ages. This comes with many different teaching resources and activities for students. This site is also intended for students' home use and it is suggested that they bookmark the site for use. The site also has a parent section designed to educate parents on the online risks, but also to enable them to help their children be safe online and give tips on the different applications they could be using.

Staff receive e-safety training on an annual basis through both sessions on inset days and with optional training sessions after Academy. This will allow staff to be aware of the risks online, and will help them to support students. This will be aimed at all staff members and will be accessible to even the least computer literate.

Any staff with any e-safety concerns should contact the technical team who will be happy to discuss any concerns or issues on a one to one basis.

4.2 Support for Students Home Use

Considering the software restrictions in place within the Academy and the staff monitoring many of the e-safety risks are minimised. Whilst issues could still occur, the obvious purpose of this document is to make this as unlikely as possible. However, students at home have very different access and in some situations, quite possibly very little monitoring from parents or carers. Computers are no longer the only way to access the internet, so it is quite possible that students could have unrestricted access to the internet on a mobile phone, a games console as well as on a personal laptop or computer.

In the Academy we will give all students an understanding of the risks involved and encourage them to transfer the skills and knowledge to their lives outside Academy. This is why it is vital that this education is well taught and thorough to have the most chance of making a sufficient impact on students. We do also try and pass this information onto parents, but this cannot be guaranteed on every occasion.

The following areas are those which are taught to students, staff and parents to help raise awareness of using the internet and its associated technologies.

4.2.1 Understanding Different Technologies

As mentioned above, e-safety does not solely concern computers. These days there are many other methods of accessing the internet and similar resources, many of which students will have access to. This section looks at the various different media which exist and some of the software which students might potentially use.

4.2.1.1 Chat Rooms

The internet is full of chat rooms but they all work in a similar way. Users can sign in (*sometimes having to register first, but not in all cases*) and are then put onto a page where users can type messages to one another. An average chat room would usually have around 20 users chatting at the same time, but this could differ between sites. Certain sites have chat rooms set to different subjects or ages, but again this differs from site to site.

In a chat room users type a message which is then sent to the room. This is displayed at the bottom of the page and scrolls upwards as other new messages appear. A message posted on a chat room is viewable to all of the users that are also signed into the chat room. As mentioned, chat rooms could be given a specified subject or age range, but there are no actual restrictions that would stop particular users. This means that it would be wholly possible for the users to be of any age, gender or nationality.

Some sites have moderators which attend rooms and audit the conversation to ensure that conversation is of a suitable level. However it is uncommon for this to a human observer, so more likely is that there will be a computer 'bot' which will be watching for inappropriate language. Anyone found to be breaching the site rules could be kicked out of the site. Depending on the site, sanctions can differ. Some sites will ban users for a few minutes after which they are allowed to return. Others might permanently ban accounts, although a user could sign up with a new account to get around this. Some sites might not have any such sanctions or moderation facilities in place, although this would be unusual.

Whilst these computer moderators provide a solution for initially blocking users, most quickly find ways of working around them. Often banned words will be misspelt, or letters, numbers or spaces inserted to break up the banned word. Other similar tactics are used to get around moderator bots, so it is generally assumed that there is no boundary on the sort of conversation that could be expected in a chat room.

Chat rooms often allow for a private chat facility where users can choose to send private messages to one another which are not displayed in the main area. This differs between sites, but is usually available in some form.

Chat rooms are most dangerous due to the casual nature of the conversation and the complete anonymity that is provided. There are no guarantees that who you are speaking to is who the person claims to be, and the conversation in chat room can involve anything, and quite often could be classed as inappropriate to minors (*depending on the site*). It is therefore important to remember on chat rooms that you cannot place too much trust in anyone or anything that is said, and they really

are only for casual conversation with others. It is particularly important to remain anonymous within a chat room (*as discussed in full in section 4.2.2*). It is possible that another user may ask for details for an Instant Messaging account to continue a conversation, for details on Instant Messaging read below.

4.2.1.2 Instant Messaging

Instant Messaging is a different type of chat interface, not unlike chat rooms. The difference with Instant Messaging is that the user only accepts the contacts they want to talk to. This ideally would include friends and family members known to them. A program is installed on the computer which constantly runs in the background and informs the user when contacts sign on to the service to let them know they are available to talk. Talking is then initiated in a similar manner to that of a private chat room.

Users can add other users by asking for their ID or email address (*depending on the software*), and then creating a friend request. Once received the other user will have to choose to accept this before the user appears on their friends list.

Instant Messaging programs also often allow extra communication features such as voice chat and even video chat using a webcam. There is also the option to transfer files, for example photos to one another.

As mentioned in the above chat room section, when using chat rooms it is quite common for users to ask for Instant Messaging contact details. This should be treated with a level of caution as this is the first step to letting someone unknown have a means of contacting you. Like all users, they would be able to see when you are online to continue a conversation. Users can however be removed or blocked.

The danger of Instant Messaging is that you could let an unknown person onto your friends list who can then contact you again and build up a level of trust. The problem being that you are never fully sure who you are talking to, and their identity. Other concerns with Instant Messaging are that many have a profile function which can have details uploaded. This is only viewable by accepted friends, but this could give an unknown user personal information about you if accepted.

Instant Messaging is a fantastic tool and can be great fun which accounts for its huge popularity. It does require a level of responsibility and care however in making sure it is used safely.

4.2.1.3 Social Networking Sites

Social Networking allows users to sign up and create their own profile consisting of name, interests, job etc. They then have a function to search for and add other users as friends. Users can then post updates in the form of messages or photos. These updates are then viewable to all of the user's friends. Depending on the site, other facilities might be enabled such as sharing photos, joining in games or opening up a live chat interface like Instant Messaging.

Social Networking is a great way to keep in touch with friends and even find lost friends by using the inbuilt search options.

Most social networking sites have a minimum age for signing up, usually around the age of 13.

However this is only based on what the user says, so it is easily possible to create an account using a made up age.

The problem with social networking sites is the amount of information that could potentially be available. The information that you put on your profile is completely up to the user, so it could be possibly for a user to go so far as to list their home address, their Academy and even their phone number. Whilst we would hope that students would not be foolish enough to go quite this far, it is certainly likely that they could be sharing information which could put them at risk.

Depending on the site being used there are different levels of access to this content. Other sites have restrictions in place so only friends can view this content, but it is often the case that users will accept all requests that they receive letting anyone have access to their profile.

It is important when using social networking sites that you only share the information that is necessary and that your profile is set to hidden so only friends can view this information. It is then important to ensure that only known friends are added as friends on your profile.

4.2.1.4 Email

Email is less used by students than some of the other methods listed here, but it is still quite likely that most students will have an email account of some kind.

Whilst there certainly could be child protection issues with email, as it is after all a method of communicating, this would probably not be the most likely method used by an online predator. Of course the same principles apply where personal information should not be shared with unknown sources and any suspicious emails should be reported.

Cyberbullying is also possible through email as messages could be sent to users. This could be done anonymously as potentially a user could sign up for a new Hotmail account entering false information for personal details. Emails from this account would then be very difficult to track back to the sender if no names were left in the message. Emails could be sent from a user's standard email address, but this would be quite foolish as these emails could be easily stored and used as proof of cyberbullying.

There are other risks when using email which are worth being aware of. Firstly there are many emails which are sent attempting to trick users into responding and sharing information such as bank account and other similar personal information. Many of these emails are setup to look like communication from banks and are produced in a very convincing manner. Users should be aware not to respond to these emails. A bank will never email to ask for any bank details, and likewise with any similar email. Email is not considered a secure medium so banks would never use such a method. Any communication that suggests this is the case is attempting to trick you.

Similarly many users will be familiar with receiving 'spam' or junk mail. This again should be avoided where possible as often it could contain files containing viruses or other similar harmful content. Any emails received like this should be deleted. To minimise the amount of junk mail received, it is important to limit the sharing of your email address. Only enter it on websites when it is absolutely necessary as many sites will pass email addresses onto third parties for use in distribution lists.

4.2.1.5 YouTube

YouTube is a hugely popular video hosting site which is used to host amateur video content. Videos can be created by a user and then uploaded from their computer to YouTube which then shares them with the world.

These days it is remarkably easy for a user to record their own film, with many users having access to basic video equipment which could include webcams, video cameras, digital cameras (*many have video functions*) and most commonly mobile phones. Movies can even be created using photos and text in programs such as Windows Movie Maker and these could also be uploaded.

YouTube does have some rules in terms of which content can be uploaded. This extends to not infringing copyright and not uploading pornographic material. After this however it is almost a case of anything goes. This can lead to some content which could be seen as inappropriate, with a chance of bad language, racism and anti-social behaviour. Unfortunately YouTube seems to be used by two distinct user bases, those that genuinely want to share something they have created with the world, and those that want to use it to upload something offensive or hurtful to another.

A problem could occur if a video is posted containing hurtful content to another student. This would be considered as a method of cyberbullying, as it would intentionally be causing upset to another student. The difficulty occurs when trying to have the content removed, as YouTube will only allow the person who uploaded the file to then remove it. If this situation arose it would have to be dealt with in Academy to ensure removal of the offending video.

4.2.1.6 Mobile Phones

With the majority of students now having access to mobile phones and many of them having full internet connections, Mobile phones carry as much risk as using a computer. The added concern is that parents may not be aware of the risk and some of the advanced features that are available on some mobile phones. There are also implications from the more conventional uses of mobile phones, like phone calls and text messaging.

As suggested, mobile phones now have the ability to run full internet applications, so all of the above (*chat rooms, social networking etc.*) could also be accessed from a mobile phone. This creates far more private access to these as it is far less likely that a family member is going to notice the content of this usage. Many parents may also not be aware that this facility exists within some modern phones.

Mobile phones can also be used as a technique in cyberbullying. Many students will have mobile phones that are carried with them at all times, so it is possible that a bully could target someone using a mobile phone at any time. For the victim it means that it is difficult to escape this bullying as it can happen at any time, so is not just limited to just being at Academy. This bullying could take place in the form of phone calls, text messages or even using the internet functions within the phone.

Another feature of advanced mobile phones is the GPS tracking system. Whilst this can be extremely useful in some circumstances, there are a few concerning issues that it raises also. This would mean, if enabled, anyone that you are friends with would be able to track you within a few hundred feet at any time when posting information. The concern being that if a student had mistakenly made friends with an online sexual predator, that they would know exactly where that student was bringing up very real issues of possible abduction.

Mobile phones are one of the key areas in dealing with e-safety in Academy as it is a medium that will be available to most students. It is also an area which comes with the most risk attached as mobile phones are used more privately than computers. Given the technology that is now available in these phones (*as suggested above*) it is vital that students understand these risks and the safe use of the technology.

4.2.1.7 Games Consoles

Most modern games consoles have a function for playing online with other users. This feature is available using the Xbox One, PlayStation 4, Nintendo Wii and also handheld consoles such as the Nintendo DS and the Sony PSP. Depending on the console, different levels of access to the internet are available. The PlayStation 4, PSP, Nintendo Wii and Nintendo DS all have online web browsing, so can connect to the internet like a normal PC (*with some software restrictions*). All the others only allow connecting to games online to play with others.

This system differs between consoles and games, but most allow a facility where communicating with others is possible and it is likely that an online game would be a target for grooming someone. Many consoles now have headsets for verbal communication whilst playing which can lead to bad or inappropriate language. Whilst video games come with an age rating on the packaging it is usually stated that they cannot guarantee the suitability of the online environment. This could include bad or intimidating language, especially in a competitive environment.

A recent popular online 'joke' is for users to join games and part way through (*when losing*) to start shouting abuse at the other player, often targeting young children. These conversations are recorded and then posted online on sites such as YouTube.

It is recommended for young users to if possible setup their own games online and to only play with trusted players (*friends*). This limits the access to other users. If playing a game with a stranger online and they do start behaving inappropriately, then simply disconnecting from the game is the best option. Depending on the console, it is possible to report players who do not meet the online rules, so sanctions can be taken against them.

Addictiveness of video games could be another potential issue, and whilst more likely with online games, could also occur on console games. It is important to ensure that children have a balanced approaching to games and that they understand when to stop playing.

4.2.1.8 Online Games

Similar in many regards to games consoles, online games are now hugely popular on PC with games boasting millions of subscribed users. There are many online games ranging from 'pay to play' titles such as World of Warcraft and Warhammer Online to 'free to play' flash games which can be found commonly across the internet.

Whilst these online games are mainly action driven with the main focus being the purpose of the game, they are also effectively huge chat interfaces with a game on top. Players communicate, work together and even fight against one another depending on the title, and this is all accompanied by a

messaging system. Most conversation comes in the form of text communication, although certain titles allow for voice chat.

Due to the public nature of online games, the concerns could be the content and language used. Whilst online games generally have moderating tools of some type like chat rooms (*see 4.2.1.1 Chat rooms for detail*s) these are not perfect and can usually be bypassed. There could also be an element of animosity especially in competitive games.

Many online games, particularly pay per play titles have full reporting functions allowing users to report other users that are acting in an inappropriate manner. This can cause them to be banned for a period of time or even permanently depending on the complaint.

Another element to online gaming is the addictive nature of many of the titles. They are often built around a mechanic whereby the longer the player plays, the further their character progresses. Some games, namely World of Warcraft would require months of playing to reach the top levels. This could become an issue as some students could become addicted, neglecting other elements of their life.

4.2.2 Sharing of Personal Information

All of the above methods of online communication come with attached risks. One of the biggest risks is internet grooming, whereby someone will use the internet as a method of making contact and befriending children. They will probably lie about themselves, making themselves younger and lie about their gender. This may occur as a one off conversation, but could result in a friendship being formed and then continued conversation. Depending on the situation this could result in a serious incident with the student possibly meeting the contact and putting themselves at risk.

This can only occur if personal information is shared with the contact, and this is where extra care needs to be taken. When using a chat room any information shared is being spread to complete strangers. Because of this it is not advisable to share any identifying information. This would include your full name (*an alias is best*), address, Academy and pictures of yourself.

The same applies for Social Networking sites such as Facebook. These sites could be accessed by anyone and it is possible that unless certain measures are taken, this information could be publically displayed. Again it is important that any user with a profile is careful with the information that it contains and the users that can access this information.

It is advisable that any student should keep their profile private. This means that only friends of the student would be able to read the information, and other users would only be able to view some very basic information. The idea would be that any information that was then shared would only be

read by other trusted users. The importance then is to ensure that only trusted users are added as friends, and not strangers from chat rooms. Depending on the Social Networking site, there are different methods to ensuring that your profile is private. Sometimes this option is not enabled by default, so must be selected.

The general rule in terms of personal information is to only give out the information that you would if approached by a stranger in the street. Don't share your full name, your address, your Academy and your personal photos, and certainly don't advertise this information to everyone, keep it private so you can choose who can see it.

4.2.3 What to do if an Issue Occurs

If any student experiences any of the potential issues as mentioned above then it is vital that the issue is reported and dealt with in the correct manner. We provide full support for our students and will help with any problems that they are encountering to the best of our ability.

If a student is using the internet at home and comes across a situation that makes them feel uncomfortable then the best recommendation is for them to remove themselves from that situation. By closing the conversation or site then they are immediately removing themselves from the situation. From there the incident should be reported in the appropriate manner. If it is due to an inappropriate website or content of a conversation then this can be reported online immediately using the ThinkUKnow Report Abuse button where full details can be logged online. This can then be followed up in Academy if necessary.

Any incidents of cyberbullying in Academy should be reported to a member of staff. Any evidence such as conversation logs, screen shots or web addresses should be gathered and given to the member of staff also. Any occasions of cyberbullying will be dealt with seriously and will be followed in-line with the Academy's behaviour policy.

If a more serious situation occurs where there is an issue of safety to a student then this should be reported immediately to the proper authorities where possible. This could include reporting to the Academy where there are trained staff at both sites to deal with disclosures of a serious nature. During our education to students we are keen to state that students should feel comfortable approaching staff members if they have any issues. As stated in section 4.1, it is important that these sessions are conducted in a correct manner should such a disclosure occur.

Any incident that is reported to the Academy will be dealt with following the correct procedure, which may include involving external agencies.

4.2.4 ThinkUKnow Website and Resources

The ThinkUKnow website (www.thinkuknow.com) is an online resource dedicated to e-safety training and support. When the page is loaded you are immediately given the choice of appropriate areas for different users. This is split into the following categories.

- 5-7
- 8-10
- 11-16
- Parent/Carer
- Teacher/Trainer

The site is designed to be as accessible as possible for students, so the different age sections are reflected in the choice of language and visual style. The content of each area is also tailored to the different users to be most relevant. The site gives full information on all of the media that could be used online and how best to stay protected when using them. It provides simple and easy to understand tips which help students to stay safe.

One of the other important elements of the site is the Report Abuse function (*CEOP Report Button*). By clicking this button the user is transferred to a page which allows them to report any online abuse that they have been a victim of. (*For example, this could be a conversation with someone online who you think might be an adult and is talking to a young person in a sexually explicit way or who is trying to meet for sex. There are also links for reporting inappropriate content on a website and for the reporting of bullying of either a conventional or cyber type. The form is easy to understand and comes with a guarantee that the report will be taken seriously.*) .

The ThinkUKnow site also acts as a great portal for adults to go and learn about the risks that could be out there for children. It is an ideal site for parents to log on to and educate themselves on the different technology and from there help to protect their children. As a parent it is possible to sign up for an account to receive email updates, and it is even possible to report abuse on behalf of a child.

For Academy's, the site is extremely valuable with some excellent resources for use by teachers. Resources include video clips, leaflets, presentations and lesson plans for dealing with a whole range of issues. Each resource is rated for a particular audience and there are many to choose from. Some of the video content is quite hard hitting and makes a strong statement. There are also links to available training for staff members.

The ThinkUKnow website is an invaluable tool for students and parents for both learning the risks and being able to report an issue. For teachers it provides great resources for teaching in Academy. We promote the site as a resource for students and parents, and as such students are being told to bookmark the site on home computers and we are also providing a link to the site on our Academy website. In the same way staff are being encouraged to have a look at the site to fully understand the features and content.

4.2.5 Cyberbullying

When people think of e-safety then they generally think of using the internet properly and being careful to avoid giving out personal information. Whilst this is a large aspect, cyberbullying is the other main area when dealing with children.

Cyberbullying is bullying, but through an electronic means. It has the same effects and the same outcomes and is usually used in conjunction with conventional bullying. However, whereas conventional bullying might take place at Academy or a specific location which would stop when the victim went home, cyberbullying can take place at any time or any place. Cyberbullying is not just limited to computers, it could also take place on mobile phones and other portable devices.

The range of methods for cyberbullying is vast, from sending emails, text messages, posting videos onto YouTube or posting on Social Networking sites. All can cause distress to the targeted individual at home as well as at Academy. Used in conjunction with conventional bullying it can make life very unpleasant for the victim.

Cyberbullying occurring in Academy is dealt with in Academy in the same way as conventional bullying, and should be reported to teachers or staff in the same way. Details of sanctions can be found in section 5.1.

Cyberbullying that occurs solely outside Academy should be reported to the appropriate outside authority. This is for parents/carers to decide. The Academy needs to be notified so that it can monitor contact between the bully and the bullied and support the student.

Almost all cyberbullying is traceable, as it is generally possible to save evidence as proof of occurrence. Instant Messaging conversations can be saved, and screenshots of abusive content can be taken and saved as evidence. It is possible however to sign up for accounts on sites and use a made up name, so it can be possible to be anonymous.

In ICT lessons students are taught to understand cyberbullying and the effects it can have. This is also covered in PSHE sessions. There are posters and information around the Academy as part of the Academy/s anti-bullying campaign.

4.26 Sexting

The transmission or exchange of indecent or inappropriate images using ICT equipment. Typically this involves the sending of a picture containing sexual images of one or more children or young person by mobile phone or computer. The image may be as part of an email, uploaded to a website or social networking site, it may have been uploaded by the subject, author or third party.

If a member of staff is made aware of a 'sexting' occurrence they should inform the Designated Safeguard Lead (*DSL*) under the normal Academy Child Protection Guidelines. The contents of advice from the DfE is given below.

"Once a teacher or other member of staff has been made aware of inappropriate images of a child or young person, they should inform the lead for the child protection in the Academy as the protection of the child or young person is paramount. He/she will liaise with the member of staff responsible for e-safety. The Academy's police liaison officer will be informed and guidance sort. Steps will be taken to preserve the image without further onward transmission. However, the image will not be deleted until local police have agreed to it."

In line with child protection procedures and with the agreement of local police, Ark Helenswood Academy will ask all the young people in possession of the image to delete it. If the image has been forwarded outside the Academy environment, we will follow the same steps to seek deletion of the image. If the image has been uploaded to any website or social networking site, we will aim to contact the provider of the service to have it removed.

Parents will be advised of the incident. It will be decided at the time whether further information or specific education is required for other students. This will depend on the timing and content of e-safety training that has already been given to students.

4.3 Parents

At Ark Helenswood Academy we feel that educating parents on the subject of e-safety is as crucial as teaching students. Whilst some parents will be aware of the technology and the risks, others might not. We try to pass as much information on to our parents as possible and offer support should they have a concern.

The main resource that we have available for parents is the Ark Helenswood Academy website. We have a separate e-safety page with full information for parents and links to other sites including the ThinkUKnow site (*see above*). Further updates can also be added here to allow parents to keep up to date.

E-safety help desks are available at Parents evenings to advertise the support we offer and we are always happy to meet with parents and discuss any issues or concerns they may have regarding their children, and will take the time out to ensure that any problems are resolved in the appropriate manner.

5. Action Taken Upon Breaching Policy

5.1 Students

Appropriate action will be taken depending on the breach of policy. In most cases this will be part of the behaviour policy, but in some cases special circumstances may apply such as being banned from using the Academy network or the internet. The latter example would need to be discussed and agreed by all staff to make it effective without hindering a student's education.

For more information on sanctions and the correct procedure for dealing with any breaches of policy, please refer to the Helenswood Academy Behaviour for Learning policy.

5.2 Staff

Any breach of policy by staff members will be dealt with in accordance with the ARK Schools Disciplinary Policy and Procedure and Disciplinary Rules. For further information on either of these documents find them attached in full in section 6.

This policy also links to:

- ARK Schools Disciplinary Policy
- Helenswood Academy Anti Bullying Policy
- Helenswood Academy Behaviour for Learning Policy
- Helenswood Academy Data Protection Policy
- Helenswood Academy Freedom of Information Policy
- Helenswood Academy Social Media Policy