**E SAFETY POLICY**

**FEBRUARY 2017**

**AUTHOR: E RIDLER**

**WMG ACADEMY FOR YOUNG ENGINEERS**

# E-SAFETY POLICY

|  |  |  |  |
| --- | --- | --- | --- |
| **Author:** | E RidlerG Jacklin | **Version:** | 3.0 |
| **Date Approved:** | February 2017 | **Date for Review:** | January 2019 |
| **Monitoring, Review and Evaluation:** KT, and Board of Governors |

1. **Introduction**

New technologies have become integral to the lives of young people in today’s society, both within the academy and in their lives outside. The requirement to ensure that users are able to access the internet, and related communications technologies, appropriately and safely is addressed within this policy and as part of the wider duty of care.

These exciting and innovative tools can be used to raise educational standards and promote learner achievement. However, the use of these new technologies can put young people at risk within and outside the academy. Some of the dangers they may face include:

* access to illegal, harmful or inappropriate images or other content;
* unauthorised access to/loss of/sharing of personal information;
* the risk of being subject to grooming by those with whom they make contact on the internet;
* the sharing/distribution of personal images without an individual’s consent or knowledge;
* inappropriate communication/contact with others, including strangers;
* cyber-bullying;
* access to unsuitable video/internet games;
* an inability to evaluate the quality, accuracy and relevance of information on the internet;
* plagiarism and copyright infringement;
* illegal downloading of music or video files;
* the potential for excessive use which may impact on the social and emotional development and learning of the young person.
* Sharing of inappropriate images even with an individual’s consent.
* The risk of being exposed to ‘extremism’ that is opposition to fundamental British values, including democracy, the rule of law, liberty, respect and tolerance.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other academy policies (e.g. Behaviour, Anti-Bullying and Safeguarding).

1. **Aims**

The aim of this policy is to build learners’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Additionally the academy will provide the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

3

The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

**3.0 Scope of the Policy**

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

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of learners when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of academy, but is linked to membership of the academy. The academy will deal with such incidents within this policy and associated behaviour that opposes Fundamental British Values and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of the academy and support agencies where appropriate.

Throughout this document there is reference made to the Acceptable Use Policy (AUP), all Users are required to accept the Acceptable Use Policy when logging in and students sign the AUP prior to starting on roll.

This policy, and associated protocols, are also applicable to staff and learners whilst on site at the adjoining Westwood Academy using mobile devices. Incidents, breaches or concerns relating to learners/staff visiting the Westwood site should immediately be reported to the Associate Principal and the Safeguarding Lead (E Ridler) as outlined in the Safeguarding Policy. The flowchart in the Appendices of the Safeguarding policy clearly outlines the involvement of the Westwood Academy Safeguarding Lead, who will be notified in each instance.

**4.0 Roles and Responsibilities**

7

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the academy:

**4.1 Governors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body will be appointed as Safeguarding Governor. The role of the Safeguarding Governor will include:

* regular meetings with the Safeguarding Lead;
* regular monitoring of e-safety incident logs;
* regular monitoring of filtering/change control logs;
* reporting to relevant Governors committee/meeting.

**4.2 Senior Leadership Team (SLT):**

* SLT is responsible for ensuring the safety (including e-safety) of members of the academy community, though the day to day responsibility for e-safety which will be delegated to the ICT and Facilities Manager;
* SLT are responsible for ensuring that the ICT and Facilities Manager, and other relevant staff, receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
* SLT will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
* SLT will receive regular monitoring reports from the ICT and Facilities Manager;
* SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. These procedures are explained at a later section.

**4.3 ICT and Facilities Manager**

8

* Reports regularly to SLT.
* Ensures the academy’s ICT infrastructure is secure and is not open to misuse or malicious attack;
* Ensures academy meets the e-safety technical requirements outlined in the WMG Academy’s AUP and any relevant Local Authority E-Safety Policy and guidance;
* Ensures users may only access the academy’s networks through a properly enforced password protection policy, in which passwords are regularly changed;
* Ensures the academy’s filtering protocol is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
* Keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
* Ensure the use of the network/remote access is regularly monitored in order that any misuse/attempted misuse can be reported to the ICT& Facilities Manager and Safeguarding Lead and reported on to the relevant reporting level as described in section 5.11 below;

9

* That monitoring software/systems are implemented and updated as agreed in academy policies.

**4.4 Teachers and Support Staff:**

Are responsible for ensuring that:

* They have an up to date awareness of e-safety matters and of the academy e-safety policy and practices;
* They have read and understood academy Acceptable Use Policy documents;
* They monitor the activity of their learners on the Virtual Learning Environment (VLE) on the courses to which they act as teachers, tutors or administrators and;
* They report any suspected misuse or problem to the relevant person as in the table below (section 5.11) for investigation/action/sanction;
* Digital communications with learners should be on a professional level and only carried out using official academy systems;
* E-safety issues are embedded in all aspects of the curriculum and other academy activities;
* Learners understand and follow the academy e-safety and acceptable use policy;
* Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
* They monitor ICT activity in lessons, extra-curricular and extended college activities;
* They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current academy policies with regard to these devices;
* In lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

**4.5 Safeguarding Lead:**

Should be trained in e-safety issues and be aware of the potential for serious learner

protection issues to arise from:

* Sharing of personal data;
* Access to illegal/inappropriate materials;
* Inappropriate on-line contact with adults/stranger;
* Potential or actual incidents of grooming;
* Cyber-bullying;
* Extremism;
* takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the academy e-safety policies/documents;
* ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
* provides training and advice for staff;
* oversees with the WMG Academy ICT technical staff including sponsors and IT support contractors;
* Receives regular reports of e-safety incidents and creates a log of incidents to inform future E-safety developments;
* Reports are reviewed and interviews conducted with students as appropriate
* meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs;
* attends relevant meetings of Governors;

**4.6 Learners:**

Are to be trained during induction and as part of their PSHE and Tutorial programmes so that they are responsible for:

* using the academy ICT systems in accordance with the Acceptable Use Policy, which they will be required to acknowledge on sign-on to academy systems before being allowed access;
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright;
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
* will be expected to know and understand academy protocols on the use of mobile phones, digital cameras and hand held devices;
* knowing and understanding academy policies on the taking and use of images and on cyber-bullying.
* Should understand the importance of adopting good e-safety practice when using digital technologies out of the WMG Academy and realise that the academy’s E-Safety Policy covers their actions out of the academy if related to their membership of the WMG Academy.

**4.7 Parents/Carers**

Parents/Carers play a crucial role in ensuring that learners understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than the learners. The WMG Academy will therefore take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website, VLE, information about e-safety campaigns, literature. Parents and carers will be responsible for:

* endorsing the academy’s Code of Conduct and Acceptable Use Policy;
* accessing the academy website/VLE in accordance with the relevant academy Acceptable Use Policy.

**4.8 Community Users**

Community Users who access the academy’s ICT systems/website/VLE as part of the Extended provision will be expected to sign a User AUP before being provided with access to the academy systems.

11

**5.0 Policy Statements**

**5.1 Education – Learners**

Whilst regulation and technical solutions are very important, their use must be balanced by educating *learners* to take a responsible approach. The education of learners in e-safety is therefore an essential part of the academy’s e-safety provision. Learners and young people need the help and support of the academy to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

* a planned e-safety programme will be provided as part of PSHE and Tutorial programme. This should be regularly revisited – this will cover both the use of ICT and new technologies in academy and outside academy;
* key e-safety messages should be reinforced as academy displays and information posters;
* learners should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;
* learners should be taught to be aware of extremism view and that they oppose Fundamental British Values;
* learners should be helped to understand the need for an Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside academy;
* learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. (Information available from Learning Resource Centre);
* rules for use of ICT systems/internet will be posted in all rooms and displayed on log-on screens;
* staff should act as good role models in their use of ICT, the internet and mobile devices.

**5.2 Education – Parents/Carers**

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of the learner and in the monitoring/regulation of the learner’s on-line experiences. Parents often either underestimate or do not realise how often learners and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The academy will therefore seek to provide information and awareness to parents and carers through letters, newsletters, web site, VLE;

**5.3 Education - Academy Enrichment Activities**

The academy will offer family learning courses in e-safety so that parents and learners can together gain a better understanding of the issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering learners to stay safe while they enjoy these new technologies, just as it is everyone’s responsibility to keep learners safe in the non-digital world.

12

**5.4 Education & Training – Staff**

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

* planned formal e-safety training will be made available to staff beginning with their Induction Programme covering Safeguarding and The WMG Academy Staff Code of Conduct. An audit of the e-safety training needs of all staff will be carried out regularly. (360 Degree Safe Self Review Tool to be used by senior staff and the Student Learner Forum). It is expected that some staff will identify e-safety as a training need within the performance management process;
* all new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the academy E-safety policy and Acceptable Use Policies;
* the ICT & Facilities Manager will receive regular updates through attendance at external training sessions and by reviewing guidance documents released by the Dfe and others;
* this E-Safety policy and its updates will be presented to and discussed by staff in staff/ team meetings/CPD days;
* the Safeguarding Lead and ICT and Facilities Manager will provide advice / guidance / training as required to individuals as required.

**5.5 Training – Governors**

Governors should take part in e-safety training/awareness sessions, with particular importance for the Safeguarding Governor. This may be offered in a number of ways:

* Attendance at training provided by the Local Authority or other relevant organization;
* Participation in academy training/information sessions for staff or parents.

**5.6 Technical – Infrastructure/Equipment, Filtering and Monitoring**

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

* the WMG Academy ICT systems will be managed in ways that ensure that the academy meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance;
* there will be regular reviews and audits of the safety and security of academy ICT systems;
* servers, wireless systems and cabling must be securely located and physical access restricted;

13

* all users will have clearly defined access rights to academy ICT systems. Details of the access rights available to groups of users will be recorded by the IT Systems technician and will be reviewed regularly (at least annually) by the governors;
* all users will be provided with a username and password and users will be required to change their password every 60 days for staff (see Acceptable User policy – security);
* generic Logons will have restricted access to the internet and must be used only when learners are under direct supervision by a teacher or member of staff. Generic logons will be used only in exceptional circumstances and will be removed at the earliest opportunity;
* the “master/administrator” passwords for the academy ICT system, used by the IT systems technician must also be available to the ICT Manager. No person will have sole access to the IT systems;
* users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
* the academy in partnership with its sponsors and IT systems contractors maintain and support a managed filtering service;
* any filtering issues should be reported immediately to the ICT Manager;
* a web filtering change log must be kept by the IT Service Provider so that in the event of needing to switch off or change the filtering (i.e. requests from staff for sites to be removed from or added to the filtered list) the ICT Manager must consider the request and if agreed they are recorded. The change log shall be reviewed regularly by the Safeguarding Governor;
* WMG Academy ICT technical staff regularly monitor and record the activity of users on the academy ICT systems and users are made aware of this in the Acceptable Use Policy and passes reports to the DSL;
* users are to report any actual / potential e-safety incident to their learning or personal tutor or other academy representative;
* appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data. Proxy servers and Firewalls, Antivirus software, internet filtering and Classroom Management software are utilised throughout;
* the provision of temporary access for “guests” (e.g. trainee teachers, visitors or business partners) onto the academy system is in place; guest accounts will be generated with access levels agreed by line managers;
* no executable files will be downloaded by users. The IT systems Technician will control the people allowed to download executable files;

14

* WMG Academy Laptops and mobile devices are to be used for academy business only. Personal use is not acceptable;
* staff are forbidden from installing programmes on academy workstations/portable devices. All users accessing academy devices will be restricted from downloading/installing software using a rights management application. Only IT Services personnel will have sufficient level of rights to allow software download/ installation;
* the use of removable media (e.g. memory sticks/CDs/DVDs) by users on academy workstations/portable devices is allowed but users are reminded of the responsibility in terms of data protection and security. See AUP/Data Protection Policy;
* the academy infrastructure and individual workstations are protected by up to date Anti-virus software. The IT Manager is responsible for ensuring this software is kept up to date;
* personal data must not be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

**5.7 Curriculum**

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

* in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
* where learners are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites visited;
* it is accepted that from time to time, for good educational reasons, learners may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation like this, staff can request that the Network/Infrastructure Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, i.e. written request (email) with clear reasons for the need and recorded;
* learners should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;
* learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

**5.8 Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

* when using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sitesstaff are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images;

15

* written permission must be sought and gained before digital images are taken and published on any externally hosted or accessible websites;
* learners must not take, use, share, publish or distribute images of others without their permission;
* care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute;
* photographs published on a website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images;
* learners’ full names will not be used anywhere on a website or blog, particularly in association with photographs;
* written permission from parents/carers of young people will be obtained before photographs of these learners are published on the academy website;
* Learner’s work can only be published with the permission of the learner and parents or carers of learners.

**5.9 Data Protection**

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

* fairly and lawfully processed;
* processed for limited purposes;
* adequate, relevant and not excessive;
* accurate;
* kept no longer than is necessary;
* processed in accordance with the data subject’s rights;
* secure;
* only transferred to others with adequate protection.

Staff must ensure that they:

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

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

* the data must be encrypted and password protected;
* the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
* the device must offer approved virus and malware checking software;

16

* the data must be securely deleted from the device once it has been transferred or its use is complete.

**5.10 Communications**

A wide range of rapidly developing communications technologies has the potential to enhance learning. The academy currently considers the benefit of using these technologies for education outweighs their risks/disadvantages. The table below identifies which technologies the Academy considers appropriate and when:-

**TABLE 1**

|  |  |  |
| --- | --- | --- |
|  | Staff & other adults | Learners |
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to academy | x |  |  |  | x |  |  |  |
| Use of mobile phones in lessons | x |  |  |  |  |  | x |  |
| Use of mobile phones in social time | x |  |  |  | x |  |  |  |
| Taking photos on mobile phones or other camera devices |  | x |  |  |  |  | x |  |
| Use of hand held devices eg PDAs, PSPs | x |  |  |  |  | x |  |  |
| Use of personal email addresses in academy, or on academy network |  |  |  | x |  |  |  | x |
| Use of academy email for personal emails | x |  |  |  |  | x |  |  |
| Use of chat rooms / facilities |  |  |  | x |  |  |  | x |
| Use of instant messaging |  |  | x |  |  |  |  | x |
| Use of social networking sites |  | x |  |  |  | x |  |  |
| Use of blogs | x |  |  |  | x |  |  |  |

**5.11 ICT Usage levels**

When using communication technologies The WMG Academy considers the following as good practice:

* the official academy email service may be regarded as safe and secure and is monitored. Staff and learners should therefore use only the academy email service to communicate with others when in academy, or on academy systems (e.g. by remote access);
* users need to be aware that email communications may be monitored;
* users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email;
* any digital communication between staff and learners or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications;
* learners will be provided with individual academy email addresses for educational use;
* learners should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material;
* personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

**5.12 Unsuitable/Inappropriate Activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution.

There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.

The WMG Academy believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below in Table 2, should not engage in these activities in or outside the academy when using academy equipment or systems. The WMG Academy policy restricts certain internet usage as follows:

**TABLE 2**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User Actions18 | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:  | accessing sexual abuse images |  |  |  |  | x |
| promotion or conduct of illegal acts, e.g. under the learner protection, obscenity, computer misuse and fraud legislation |  |  |  |  | x |
| adult material that potentially breaches the Obscene Publications Act in the UK |  |  |  |  | x |
| criminally racist material in UK |  |  |  |  | x |
| pornography |  |  |  |  | x |
| promotion of any kind of discrimination |  |  |  | x |  |
| promotion of racial or religious hatred  |  |  |  |  | X |
| threatening behaviour, including promotion of physical violence or mental harm  |  |  |  |  | x |
| any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute |  |  |  | x |  |
|  | Information that is extremist in nature and opposed Fundamental British Values |  |  |  |  | x |
| Using WMG Academy systems to run a private business |  |  |  | x |  |
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed the academy |  |  |  | x |  |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions |  |  |  | x |  |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) |  |  |  | x |  |
| Creating or propagating computer viruses or other harmful files |  |  |  | x |  |
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet |  |  |  | x |  |
| On-line gaming (educational)  |  | x |  |  |  |
| On-line gaming (non educational) |  |  |  | x |  |
| On-line gambling |  |  |  | x |  |
| On-line shopping / commerce |  |  |  | x |  |
| File sharing |  | x |  |  |  |
| Use of social networking sites |  | x |  |  |  |
| Use of video broadcasting e.g. YouTube19 |  | x |  |  |  |

**5.12 Responding to incidents of misuse**

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

If any apparent or actual misuse appears to involve illegal activity as outlined above i.e. table 2

Then the ICT& Facilities Manager or a member of the SLT must be informed immediately and advice sought from the police working in conjunction with the IT systems technician to preserve evidence and prevent further illegal activity.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In this case an investigation in conjunction with the Safeguarding Lead and the IT Manager will be carried out.

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

20

Listed below in Table 3.1 and 3.2 are the responses that will be made to any apparent or actual incidents of misuse:

**TABLE 3.1**

|  |  |
| --- | --- |
| **Learners**  | **Actions/Sanctions**  |
| Incidents:Continued actions will necessitate escalation of reporting | Refer to lead teacher  | Refer to Curriculum Lead | Refer to SLT/Director of Operations | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg. Principal’s Detention, Internal / external exclusion  |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). |  | x | x | x | x | x | x | x | x |
| Unauthorised use of non-educational sites during lessons. | x | x |  |  | x | x | x | x |  |
| Unauthorised use of mobile phone / digital camera / other handheld device | x |  |  |  |  |  |  | x |  |
| Unauthorised use of social networking / instant messaging / personal email | x |  |  |  |  |  |  | x |  |
| Unauthorised downloading or uploading of files | x | x |  |  | x | x | x | x |  |
| Allowing others to access academy network by sharing username and passwords | x |  |  |  |  |  |  | x |  |
| Attempting to access or accessing the academy network, using another learners’s account | x | x | x |  |  | x | x | x | x |
| Attempting to access or accessing the academy network, using the account of a member of staff | x | x | x |  | x | x | x | x | x |
| Corrupting or destroying the data of other users | x | x | x |  | x | x | x | x | x |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | x | x | x |  | x | x | x | x | x |
| Continued infringements of the above, following previous warnings or sanctions |  |  |  | x |  |  |  |  |  |
| Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy |  | x | x |  |  | x | x | x | x |
| Using proxy sites or other means to subvert the academy’s filtering system |  |  | x |  | x | x | x | x | x |
| Accidentally accessing offensive or pornographic material and failing to report the incident | x | x |  |  |  |  |  | x |  |
| Deliberately accessing or trying to access offensive or pornographic material | x | x | x |  | x | x | x | x | x |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act21 | x | x | x |  |  | x |  | x | x |
| Deliberately accessing, or trying to access ‘extremist’ information that opposes Fundamental British Values | x | x | x | x | x | x | x | x | x |

**TABLE 3.2**

|  |  |
| --- | --- |
| **Staff** | **Actions / Sanctions**  |
| Incidents:Continued actions will necessitate increased levels of reporting  | Refer to line manager | Refer to Curriculum Lead | Refer to SLT/Facilities Manager | Refer to Police/LADO considered | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). |  |  | x | x | x | x | x | x |
| Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email | x | x | x |  |  | x |  |  |
| Unauthorised downloading or uploading of files | x | x | x |  | x | x |  |  |
| Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person’s account | x | x | x |  |  | x |  | x |
| Careless use of personal data eg holding or transferring data in an insecure manner | x | x | x |  |  | x |  |  |
| Deliberate actions to breach data protection or network security rules |  |  | x |  | x | x | x | x |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software |  |  | x | x |  | x | x | x |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature |  |  | x | x |  | x | x | x |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with learners  | x | x | x |  |  | x | x | x |
| Actions which could compromise the staff member’s professional standing  |  | x | x |  |  | x |  |  |
| Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy |  |  | x |  |  | x | x | x |
| Using proxy sites or other means to subvert the academy’s filtering system |  | x | x |  | x | x | x | x |
| Accidentally accessing offensive or pornographic material and failing to report the incident |  | x |  |  |  |  |  | x |
| Deliberately accessing or trying to access offensive or pornographic material |  | x | x | x | x | x | x | x |
| Breaching copyright or licensing regulations |  |  | x |  |  |  | x | x |
| Continued infringements of the above, following previous warnings or sanctions |  |  | x |  |  |  | x | x |
| Deliberately accessing, or trying to access ‘extremist’ information that opposes Fundamental British Values | x | x | x | x | x | x | x | x |

1. **Monitoring, Review and Evaluation**

**6.1 Schedule for Development/Monitoring/Review**

|  |  |
| --- | --- |
| This e-safety policy was approved by Governors on: | TBA |
| The implementation of this e-safety policy will be monitored by the: | Relevant committee of the Governing Body through the ICT Manager and Safeguarding Lead |
| Monitoring will take place at regular intervals: | Annually |
| Governors will receive a report on the implementation of the e-safety policy which will include anonymous details of e-safety incidents | Annually |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | Next scheduled Review date January 2018  |
| Should serious e-safety incidents take place, the following persons / agencies should be informed: | ICT ManagerSafeguarding LeadSafeguarding Lead at The Westwood Academy if an incident occurs on the adjoining siteSenior Leadership TeamPolice  |

The academy will monitor the impact of the policy by:

* monitoring logs of reported incidents
* monitoring logs of internet activity (including sites visited)
* Internal monitoring of network activity
* 360 Degree Safe Self Review Tool
* Surveys/questionnaires of
	+ Learners (e.g. CEOP ThinkUknow survey)
	+ Parents/Carers
	+ Staff