NOBLE HALL
Leadership Academy For Girls

E-Safety Policy

September 2017

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in the Academy for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside the Academy. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and learners learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the Academy are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in the Academy and at home has been shown 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 or 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.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other Academy policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, 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.

The Academy provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the Academy intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope

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

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the Academy.

NOBLE HALL
Leadership Academy For Girls

Board of Directors

Board of Directors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A member of the Board of Directors, TBC, has taken on the role of E-Safety Director. The role of the E-Safety Governor will include:

- Meetings with the ICT coordinator and the Principal
- Regular monitoring of e-safety incident logs
- Monitoring of filtering/change control logs
- Reporting to the Board of Directors.

Principal & Senior Leadership Team (SLT)

The Principal is responsible for ensuring:

- The safety (including e-safety) of all members of the Academy community, although the day to day responsibility for e-safety will be delegated to the ICT coordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the Academy e-safety policies and documents (in conjunction with e-safety co-ordinator)
- The Academy's Designated Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

ICT Coordinator

The ICT Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, ICT Technical staff, E-Safety Director and SLT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Providing training and advice for staff;
- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programme in the Academy

In addition the ICT Coordinator is responsible for ensuring that:

- The Academy's ICT infrastructure is secure and meets e-safety technical requirements
- The Academy's password policy is adhered to
- The Academy's filtering policy is applied and updated on a regular basis
- Co-ordinator keeps up to date with e-safety technical information
- The use of the Academy's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Principal for investigation/action/sanction.

Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices
- They have read, understood and signed the Academy Staff Acceptable Usage Policy (AUP)
- E-safety issues are embedded in all aspects of the curriculum and other Academy activities
- Learners understand and follow the Academy's e-safety and acceptable usage policies
- Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended Academy activities

- In lessons where Internet use is 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.

Learners (to an age appropriate level)

- Are responsible for using the Academy ICT systems in accordance with the Learner Acceptable Usage Policy, which they will be required to sign before being given access to the Academy systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of the Academy and realise that the Academy's e-safety policy also covers their actions out of the Academy, if related to their membership of the Academy.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children 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 their children. The Academy will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Learner Acceptable Usage Policy.
- Accessing the Academy website in accordance with the relevant Academy Acceptable Usage Policy.

Education and Training

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

- A planned e-safety programme is provided as part of the house tutor and assembly programme and is regularly revisited in Information Communication Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in the Academy and outside of the Academy.
- Learners are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Learners are helped to understand the need for the Learner AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of the Academy.
- Learners are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Usage Policy (see Appendix 5/6)

- Parents/carers will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- Staff and regular visitors to the Academy have an AUP that they must read through and sign to indicate understanding of the rules.

Copyright

- Learners to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations - staff to monitor this.
- Learners are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright.

NOBLE HALL
Leadership Academy For Girls

Staff Training

- ICT coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- A planned programme of e-safety training is available to all staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy E-Safety policy, Acceptable Usage and Child Protection Policies.

Commmunication

Email

- Digital communications with learners (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official Academy systems.
- The Academy's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, the Academy curriculum systems);
- Under no circumstances should staff contact learners, parents/carers or conduct any Academy business using personal e-mail addresses.
- The Academy e-mail is not to be used for personal use. Staff can use their own email in the Academy (before, after the Academy and during lunchtimes when not working with children) – but not for contact with parents/ learners.

Mobile Phones

- The Academy mobile phones only should be used to contact parents/carers.
- Staff should not be using personal mobile phones in the Academy during working hours when in contact with children.
- Learners are not permitted to bring a mobile phone or any mobile device into the Academy.

Social Networking Sites

Young people will not be allowed on social networking sites at the Academy; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- Staff should not access social networking sites whilst on the premises.
- Staff users should not reveal names of staff, learners, parents/carers or any other member of the Academy community on any social networking site or blog.
- Learners/Parents/carers should be aware the Academy will investigate misuse of social networking if it impacts on the well-being of other learners or stakeholders.
- If inappropriate comments are placed on social networking sites about the Academy or the Academy staff then advice would be sought from the relevant agencies, including the police if necessary.

Digital Images

- The Academy record of parental permissions granted/not granted must be adhered to when taking images of our learners. A list can be obtained from reception.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Principal.
- Where permission is granted the images should be transferred to the Academy storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.
- Permission to use images of all staff who work at the Academy is sought on induction and a copy is located in the personnel file.

Although many of the above points are preventative and safeguarding measures, it should be noted that the Academy will endeavour whenever possible to use social networking in positive ways to publicise, inform and

communicate information. The Academy has an active website and twitter account which are used to inform, publicise Academy events and celebrate and share the achievement of learners.

Removable Data Storage Devices

- Only the Academy provided removable media should be used
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using the Academy provided anti-virus software before run, opened or copied/moved on to local/network hard disks.
- Learners should not bring their own removable data storage devices into the Academy unless asked to do so by a member of staff.

Websites

- In lessons where Internet use is 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.
- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are not allowed when working with learners in Years 7 and 8 who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents will be advised to supervise any further research.
- All users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which learners are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the learners on the internet by the member of staff setting the task. All staff are aware that if they pass learners working on the internet that they have a role in checking what is being viewed. Learners are also aware that all internet use at the Academy is tracked and logged.
- The Academy only allows the ICT co-ordinator and the Senior Leadership Team access to Internet logs.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Learners

- Should only let the Academy staff know their Academy passwords.
- Inform staff immediately if passwords are traced or forgotten.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the Academy's network without the specific permission of the Principal.
- Learners should not bring in their own equipment unless asked to do so by a member of staff.

Use of The Academy Equipment

- No personally owned applications or software packages should be installed on to the Academy ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.

- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the Academy's Internet access is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up by the ICT coordinator and/or members of the Senior Leadership Team depending on the severity of the incident.

- ICT coordinator will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the Academy who comes across an e-safety issue does not investigate any further but immediately reports it to the ICT coordinator and impounds the equipment. This is part of the Academy safeguarding protocol. (If the concern involves the ICT coordinator then the member of staff should report the issue to the Principal).

Incident Reporting

Any e-safety incidents must immediately be reported to the Principal (if a member of staff) or the ICT Coordinator (if a learner) who will investigate further following e-safety and safeguarding policies and guidance.

Responding to incidents of misuse

It is hoped that all members of the 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. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. 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 as follows (Appendix 3 for learners and Appendix 4 for staff respectively).

Appendix 1

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Academy currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and other adults				Students and young people			
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones								

May be brought to the Academy									
Mobile phones used in lessons									
Use of mobile phones in social time									
Taking photographs on mobile devices									
Use of PDAs and other educational mobile devices									
Use of the Academy email for personal emails									
Social use of chat rooms/facilities									
Use of social network sites									
Use of educational blogs									

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

- The 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 the Academy, or on the 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, Learning Platform 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 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.

NOBLE HALL
Leadership Academy For Girls

Appendix 2

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the 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, either because of the age of the users or the nature of those activities. The Academy believes that the activities referred to in the following section would be inappropriate and that users, as defined below, should not engage in these activities in the Academy or outside the Academy when using the Academy equipment or systems. The Academy policy restricts certain internet usage as follows. 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:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					
Adult material that potentially breaches the Obscene Publications Act in the UK					
Criminally racist material in the UK					
Pornography					
Promotion of any kind of discrimination					
Promotion of racial or religious hatred					
Threatening behaviour, including promotion of physical violence or mental harm					
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					
Using the Academy systems to run a private business					
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Academy					
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					

Creating or propagating computer viruses or other harmful files					
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					

Appendix 3

The guidance in this policy should be implemented with cross reference to the Academy's Child Protection, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

Appendix 4

Incidents involving members of staff	Refer to the Principal *See below	Refer to technical support staff for action re filtering, security etc	Potential Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email			
Unauthorised downloading or uploading of files			
Allowing others to access the Academy network by sharing username and passwords or attempting to access or accessing the Academy network, using another person's account.			
Careless use of personal data e.g. holding or transferring data in an insecure manner			
Deliberate actions to breach data protection or network security rules			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software			

NOBLE HALL
Leadership Academy For Girls

Incident involving learners	Teacher to use the Academy behaviour policy to deal with	Refer to Leader Tutor	Refer to police	Refer to technical support staff for action re security/filtering etc
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities).		. . . .	. . . .	. . . .
Unauthorised use of non-educational sites during lessons	. . .			. . .
Unauthorised use of mobile phone/ digital camera/ other handheld device.	. . .			.
Use of social networking/ instant messaging/ personal email	. . .	. . .		. . .
Unauthorised downloading or uploading of files		. .		. .
Allowing others to access the Academy network by sharing username and passwords		. . .		. . .
Attempting to access or accessing the the Academy network, using another student's account		. . .		. . .
Attempting to access or accessing the Academy network, using the account of a member of staff		. . .		. . .
Corrupting or destroying the data of other users		. .		. .
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		. . . .		. . . .
Continued infringements of the above, following previous warnings or sanctions		. . . .	.	. . . .

NOBLE HALL
Leadership Academy For Girls

Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy				
Using proxy sites or other means to subvert the Academy's filtering system				
Accidentally accessing offensive or pornographic material and failing to report the incident				
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature				
Using personal email/ social networking/ instant messaging/ text messaging to carry out digital communications with learners				
Actions which could compromise the staff member's professional standing				
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy				
Using proxy sites or other means to subvert the the Academy's filtering system				
Deliberately accessing or trying to access offensive or pornographic material				
Breaching copyright or licensing regulations				
Continued infringements of the above, following previous warnings or sanctions				

*In event of breaches of policy by the Principal, refer to the Chair of Directors.

NOBLE HALL
Leadership Academy For Girls

Appendix 5

Acceptable Internet Use Policy – Students

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the Academy network through my authorised username and password. I will not use the passwords of others.
- I will not use the Academy IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any Academy computer or try to alter computer settings.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Signed ……..

Date …….

NOBLE HALL
Leadership Academy For Girls

Appendix 6

Acceptable Internet Use Policy – Staff and Volunteers

New technologies have become integral to the lives of children and young people in today's society, both within the Academy and in their lives outside the Academy. The Internet and other digital information and communications are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe Internet access at all times.

This policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- All ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to improve learning opportunities for all and will, in return, expect staff and volunteers to agree to be responsible users.

Responsible Use Agreement

I understand that I must use the Academy ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with learners.

For my professional and personal safety:

- I understand that the the Academy will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the Academy ICT systems (e.g. laptops, email, Learning Platform etc).
- I understand that the Academy ICT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the Academy.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person (see policy flowcharts).

I will be professional in my communications and actions when using the Academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Academy's policy on the use of digital/video images. I will not use chat and social networking sites in the Academy in accordance with the Academy's policies.
- I will only communicate with learner and parents/carers using official Academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using the Academy's equipment. I will also

follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the Academy ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in the Academy policies.
- I will not disable or cause any damage to the Academy equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for the Academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the Academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of ICT equipment in the Academy, but also applies to my use of the Academy ICT systems and equipment out of the Academy and my use of personal equipment in the Academy.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Board of Directors and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the ICT systems (both in and out of the Academy) and my own devices (in the Academy and when carrying out communications related to the Academy) within these guidelines.

Staff/Volunteer

Name ……..

Signed …….

Date ……