	E-Safety Policy	Author:	James Done
		Approved by:	Vivien Sharples
		Date:	12 December 2017
		Review date:	December 2018

CONTEXT

The Academy has statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside Academy. Due to the ever changing nature of digital technologies, the Academy reviews its E-Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place. The policy is reviewed in consultation with the Academy community through a range of formal and informal meetings

SCOPE OF THE POLICY

This policy applies to all members of the Academy community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Academy ICT systems, both in and out of the Academy. Academy staff are given specific guidance in the latter part of this policy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students 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 outside of the Academy, but is linked to membership of the Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix 1 for searching of devices and deletion of data). The will deal with such incidents identified within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate E-Safety behaviour that take place out of Academy.

ROLES AND RESPONSIBILITIES

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the Academy.

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 Governor will be responsible. The role of the E-Safety Governor will include:

- regular meetings with the Safeguarding Lead / E-Safety Coordinator
- regular monitoring of E-Safety incident logs
- reporting to relevant Governors' meeting.

Principal and Leadership Team:

- The Principal has a duty of care for ensuring the safety (including E-Safety) of members of the Academy community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator/Safeguarding Lead.
- The Principal and another member of the Leadership Team 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.
- The Principal is responsible for ensuring that the Safeguarding Lead/E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator/ Safeguarding Lead.

Designated Safeguarding Lead:

- Should be trained in E-Safety issues.
- Should aware of the potential for serious child protection/safeguarding issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying.
- 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, parents/carers and students, in conjunction with the E-safety Co-ordinator.
- Liaises with the Local Authority/relevant body.
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments).
- Meets with a staff / student E-Safety group at regular intervals to develop strategy.
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meetings of Governors.
- Reports regularly to Leadership Team.

E-Safety Co-ordinator:

- Takes day to day responsibility to ensure E-Safety issues are effectively dealt with and has a leading role in establishing and reviewing the Academy E-Safety policies/documents.
- Liaises with Academy technical staff.
- Should be trained in E-Safety issues.
- Ensures the provision of E-safety education within the curriculum.
- Should aware of the potential for serious child protection/safeguarding issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying.
- Works closely with the Safeguarding Lead.

Network Manager/Technical Staff should be responsible for ensuring that:

- the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- the Academy meets required E-Safety technical requirements and any Local Authority E-Safety Policy or Guidance that may apply
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- they keep 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
- the use of the network is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety coordinator for investigation/action/sanction
- monitoring software are implemented and updated as agreed in Academy policies.

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
- they have read, understood and signed the Staff Acceptable Use Policy (appendix 2)
- they report any suspected misuse or problem to the Principal, E-Safety Co-ordinator or Safeguarding Lead for investigation/action/sanction
- all digital communications with students, parents/carers 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 activities
- students understand and follow the E-Safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other Academy activities (where allowed) and implement current policies with regard to these devices.

Students:

- are responsible for using the Academy digital technology systems in accordance with the Student Acceptable Use Policy (see appendix 3)
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good E-Safety practice when using digital technologies out of Academy and realise that the Academy's E-Safety Policy covers their actions out of 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. The Academy will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, website and VLE. Parents/carers will be encouraged to support the Academy in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Academy events
- access to parents'/carers' sections of the website/VLE and on-line student records
- their children's personal devices in the Academy

POLICY STATEMENTS

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / to take a responsible approach. The education of students in E-Safety is therefore an essential part of the Academy's E-Safety provision. Children and young people need the help and support of the Academy to recognise and avoid E-Safety risks and build their resilience.

E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-Safety curriculum will be provided as part of ICT and PHSE and will be regularly revisited.
- Key E-Safety messages will be reinforced as part of a planned programme of assemblies and tutorial activities.
- Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

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 their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across

potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents'/Carers' evenings
- High profile events & campaigns

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:

- A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process.
- All new staff will receive E-Safety training as part of their induction programme, ensuring that they fully understand the Academy E-Safety policy and acceptable use agreements.
- The E-Safety Co-ordinator or Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff.
- E-Safety Co-ordinator or Safeguarding Lead will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in E-Safety training/awareness sessions, with particular importance for those who are involved in E-Safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority.
- Participation in Academy training/information sessions for staff, parents/carers or students.

Technical – infrastructure/equipment, filtering and monitoring

The Academy will be responsible for ensuring that the Academy 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:

- Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of Academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to Academy technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The "administrator" passwords for the Academy ICT system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. Academy safe)
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Academy technical staff regularly monitor and record the activity of users on the Academy technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/ security breach to the Network Manager, via the ICT support icon on staff computers or in person if there is an immediate safeguarding issue.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the Academy systems and data. These are tested regularly. The Academy infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers,) onto the Academy systems.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on Academy devices.
- This policy should be read in conjunction with the CCTV (Closed Circuit Television) policy.

USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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 sites.
- Staff and volunteers 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. Images can be taken on personal devices for publicity/teaching and learning purposes only. These should be transferred to Academy network/Administration Assistant (Publicity/ Communications) as soon as possible and then deleted from personal device.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Parents/carers of new students are notified that we may use photographs of students unless they inform us in writing that they do not wish this to happen.
- Please refer to the CCTV policy for details of CCTV procedures.

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.

The Academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function; it will not hold it for longer than necessary; and it will only for used for the purposes for which it was collected.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

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:

Students are allowed to bring mobile phones, tablets or gaming devices into Academy at their own risk. Mobile phones are not normally allowed to be switched on in lessons, unless permission is given by the teacher for a specific purpose. Mobile phones are allowed outside the building, in the social areas and in the dining hall/cafeteria before Academy, at break and at lunch.

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

- The email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Students must immediately report to a member of staff any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, chat, VLE etc) must be professional in tone and content.
- Students should be taught about E-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff.

UNSUITABLE/INAPPROPRIATE ACTIVITIES

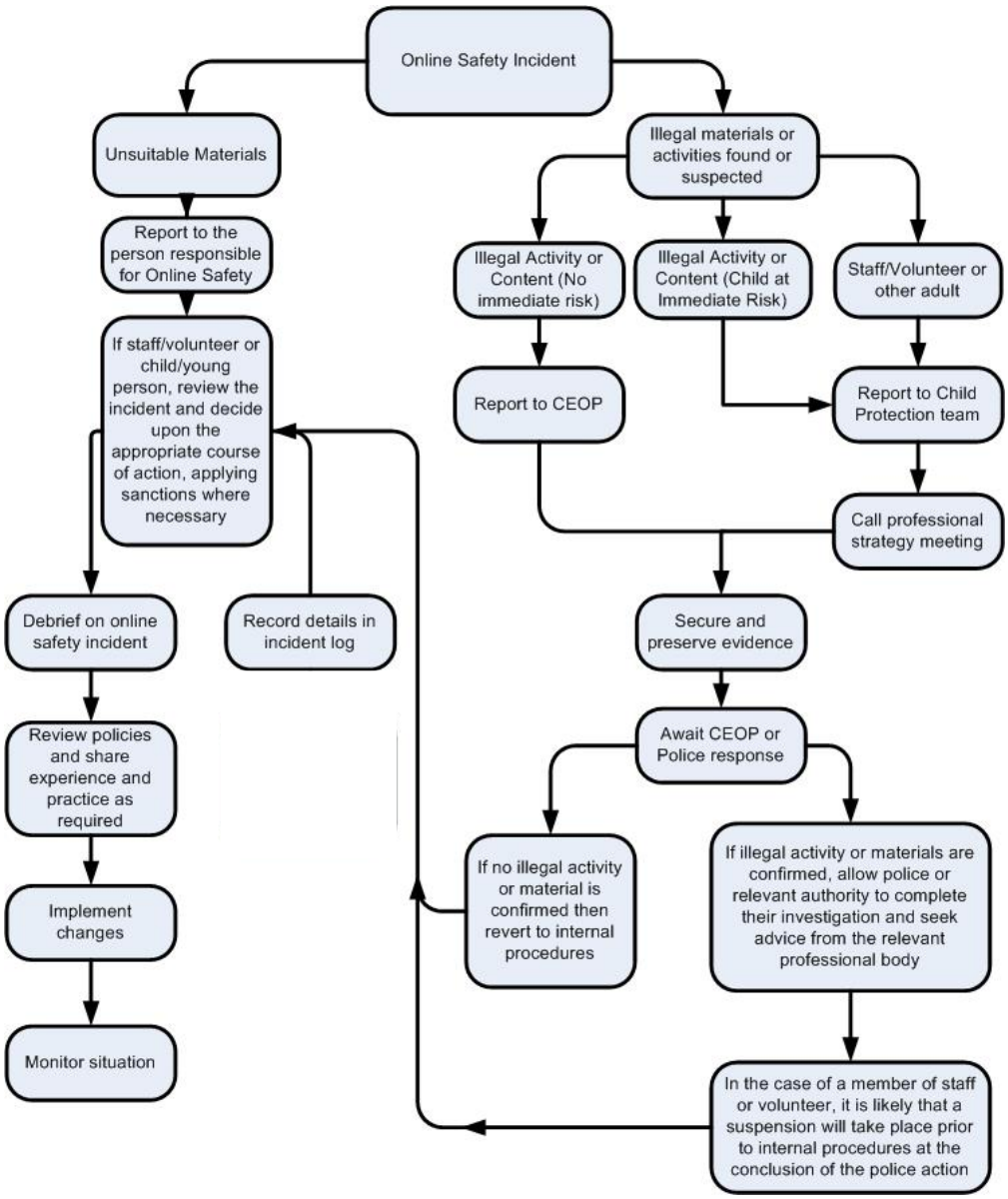
Students shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: child sexual abuse images, grooming, incitement, arrangement or facilitation of sexual acts against children, possession of pornographic images, criminally racist material, promotion of any kind of discrimination, 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.

They should also not reveal or publicise confidential or proprietary information, create or propagate computer viruses or other harmful files, infringe copyright, use systems, applications, websites or other mechanisms that bypass the filtering systems.

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by Local Authority or national/local organisation
    - police involvement and/or action.
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the Academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

Academy Actions & Sanctions

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. Sanctions can involve warnings, removal of network or internet access rights, informing parents/carers and further sanctions such as detentions and exclusions where deemed appropriate by the Academy.

When a student is found to be deliberately accessing or trying to access material that could be considered illegal, the Principal should be aware and the incident referred to the police.

STAFF ACCEPTABLE USE OF ICT POLICY

INTRODUCTION

The Academy's IT resources are essential to the effective delivery of educational provision. Computers and other networked facilities, including internet access, are available to staff and students within the Academy and should be used to promote educational learning. It is therefore vital that all staff, agents and contractors are aware of the Academy's policies and procedures relating to the use of IT resources. A poorly administered network or weak password controls could expose the Academy's information to an unauthorised user or introduce a virus infection.

SCOPE

- This policy applies to all technology and communications equipment provided by Derbyshire County Council/Academy (e.g. PCs, devices, tablets, mobile phones with internet access etc).
- Any personal or potentially personal information sent via e-mail and the Internet is covered by the Data Protection Act 1998. The Act requires all employees to take special care when handling personal information.
- Emails may be covered by the Freedom of Information Act and are disclosable as part of legal proceedings. Employees should exercise the same caution when writing emails as they would in more formal correspondence.
- Use of email and the internet, which brings the County Council/Academy into disrepute, may result in disciplinary action.
- Limited use of the internet and email is permitted subject to these principles:
    - Email: employees are allowed limited use of e-mail for personal communication
    - Internet: personal use of the internet is permitted outside normal working hours
    - Any personal use must not, in any way, distract employees from the effective performance of their duties
- This policy should be read in conjunction with the CCTV policy.

USE OF INTERNET AND ELECTRONIC COMMUNICATION

Internet and electronic communication use is integral to the effective delivery of educational services provided by the Academy. Electronic communication can include emails, text messages and social media apps. Nothing in this policy should be read as restricting the proper use of communication and internet for Academy activities. Limited personal use of Academy's internet and message systems is permitted subject to these principles and guidance notes.

- Where possible, personal use of electronic communication should be in employees' own time. Limited use during the working day is allowed, but should be restricted to a few minutes a day to respond to urgent incoming messages and **should not be used when teaching or supervising students.**

  Excessive use of electronic communication is **not allowed** and **may result in disciplinary action.**

- While personal use of the internet and electronic communication is permitted during lunch breaks and out of working hours, staff should be aware that the facilities are provided by the Academy and any activity received/sent through the Academy's network, personal or otherwise, is recorded and will be monitored.

- Staff should not engage in 'recreational' chatting during working time, on email, text or through instant messaging, that results in lost productivity or distracts other employees from their work. The Academy's facilities must never be used for the passing of inappropriate personal information of any kind.

- Electronic communication is now used widely to communicate both internally and externally, providing rapid circulation and many positive benefits. Staff should, however, remain aware of their professional position when communicating electronically. When email is used to communicate with students, parents or carers as part of a professional role, a Academy email address should always be used. The style and format of any such communication should follow guidelines provided by the Academy. Staff should consider whether it is advisable to copy a colleague into any contact with a student or parent as a further safeguard. Staff should be aware that email is not always the best form of communication and should consider alternatives, as appropriate.

- Improper statements in electronic communication can give rise to personal liability and liability for the Academy and may constitute a serious disciplinary matter. Electronic communication that may embarrass misrepresent or convey an unjust, or unfavourable, impression of the Academy or its business affairs, employees, suppliers and their families are not permitted.

- Extreme care must be taken when using the Academy's email facilities to transmit information. Confidential or sensitive information should not be sent via the internet or email unless the data is protected by the Academy's secure provision for such communications. Staff should remember that when a Subject Access Request or Freedom of Information request is submitted relevant email communications will be included in the material to be provided.

- Employees must not use electronic communication in any way that is insulting or offensive.

  Employees must not deliberately view, copy or circulate any material that:

  - could constitute bullying
  - is sexually explicit or obscene
  - is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
  - contains material the possession of which would constitute a criminal offence
  - promotes any form of criminal activity
  - contains unwelcome propositions
  - contains images, cartoons or jokes that will cause offence
  - appears to be a chain letter.

- Personal use of internet

  - Use of the internet should be limited to employees' own time except in exceptional circumstances.

- Use of the internet via County Council or Academy equipment should exclude use for trading or personal business purposes.
- Use of the internet to buy goods or services will not render the County Council or Academy liable for default of payment or for the security of any personal information disclosed. Staff are advised not to use the Academy's computer system for making payments.

- Site Contents

  Many internet sites contain unacceptable contents. Employees must not deliberately view, copy or circulate any material that:

  - is sexually explicit or obscene
  - is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
  - contains material, the possession of which would constitute a criminal offence
  - promotes any form of criminal activity
  - contains images, cartoons or jokes that will cause offence
  - that constitutes bullying.

- Accidental Access to Inappropriate Material

  Many internet sites that contain unacceptable content are blocked automatically by the Academy's filtering systems. However it is not possible to block all 'unacceptable' sites electronically in all circumstances. If staff become aware of any sites that require re-categorisation they should inform the Academy's IT technician as soon as possible. Employees may receive an e-mail or visit an internet site that contains unacceptable material. If this occurs, a line manager or the Principal should be informed as soon as possible. The Principal will use their professional judgement whether to report the matter further. In this situation the staff member should ensure a short written record is kept as they may be asked to provide details relating to the incident and an explanation of how it occurred. This information may be required later for management or audit purposes.

- Copyright

  Employees may be in violation of copyright law if text is simply cut and pasted into another document. This may equally apply to photographs and music samples used as illustration or backing track in resource materials. Teachers should make it clear to students that care should be taken when including this type of material in any Academy or exam work. Most sites contain a copyright notice detailing how material may be used. If in any doubt about downloading and using material for official purposes, legal advice should be obtained. Unless otherwise stated on the site all down loaded material must be for curricular or research purposes and must not be passed to third parties.

  Downloading of video, music files, games, software files and other computer programs – for non-work related purposes-is not allowed. These types of files consume large quantities of storage space on the system and may violate copyright laws.

Safe Working Practice

- Staff should make careful, considerate use of the Academy's IT resources, report faults and work in a way that minimises the risk of introducing computer viruses into the system.
- Staff are responsible for maintaining the security of computers and networks by only using their own logon details and not allowing other staff or students to use their personal passwords. Staff should ensure that machines are not left unattended when they are logged on.
- Staff should ensure as far as possible, that when using work equipment at home, other family members do not use the equipment for their personal use. Staff are responsible for all the content (software and data) on any equipment allocated to them.
- Staff should not install any unlicensed software on machines allocated to them.
- Staff must make every endeavour to protect students from harmful or inappropriate material accessible via the internet or transportable on computer media.

365 Learning Platform

- The 365 Learning Platform provides 24 hour access to a wide range of information – including resource materials, student data and Academy policies. It is essential that clear guidelines are in place.

- The Network Manager has a duty to ensure that the site access is secure with passwords providing differing levels of access to staff and students.
- There must be no expectation by the Academy that staff will be available outside normal working hours just because they are able to access the 365 Learning Platform from home. There will therefore be no expectation, other than by agreement, that staff will respond to email or other messages, sent outside the working day, before the start of the next working day. It will be made clear to parents that if students are posting work on the site, or emailing work directly to a member of staff, that there must be no expectation of an immediate response.
- Access to the 365 Learning Platform from outside the Academy should not be a reason to reduce timescales for completion of work by either staff or students. For example, the same amount of time should be allowed for completion of annual reports if done on-line through the 365 Learning Platform as that allocated previously for hand-written reports.

Social Media

- For the purpose of this policy social media is a type of interactive online media that allows parties to communicate instantly with each other, or to share data in a public forum. This includes online social forums such as Twitter, Facebook, LinkedIn, internet newsgroups, and chat rooms. Social media also covers blogs and video- and image-sharing websites such as YouTube and Flickr.

  There are many more examples of social media than can be listed here and this is a constantly changing area. These guidelines should be followed in relation to any social media used.

  The use of sites such as Facebook, Snapchat, Instagram, Twitter, and many others (such as on-line gaming through Xbox or PlayStation live) is now increasingly widespread. However, as well as bringing many positive benefits, there are also many potential problems. The following guidance is given to all staff and students for their own protection. The guidance should apply whether the staff member is using Academy hardware or their own personal hardware (computer, phone, console etc.)

- At all times, staff should be aware of the Academy's Code of Conduct expected of professional adults working with children. Employees who work directly with members of the public, including parents, need to be aware that the information they post on their profile can make them identifiable to members of the wider Academy community as well as people they know in a private capacity.

  Employees should therefore consider this when setting up their profile, particularly in relation to; the use of a photograph, providing details of their occupation, employer and work location.

  Staff should consider very carefully any conflict of interest when linking through social media to people they also know through work. The Academy considers it would be inappropriate to have students as 'friends' through social media, and consequently, to do so may be considered to be a disciplinary matter.

  Online sites such as Facebook are in the public domain, and personal profile details can be seen by anyone, even if users have their privacy settings on the highest level. Also if a user's profile is linked to other sites, any changes to their profile will be updated there too. Staff who have set their privacy level to the maximum can have their privacy compromised by 'friends' who may not have set their security to the same standard and therefore comments, photographs or video clips sent to such contacts may be more widely available than originally anticipated.

- Staff should be aware of the image they are presenting when communicating via such media and ensure, as far as possible, that any comments made are not open to misinterpretation. Circulation of comments on such media can be rapid and widespread and therefore staff should be encouraged to adopt the general premise of not putting anything on such a site (or in an email) that they would not put in a formal letter, be prepared to say in a face-to-face conversation or discuss in a public place.

- The Principal and Governors will give consideration, when reaching decisions relating to potential disciplinary cases for breach of such a code, to the difficulty of staff members in 'controlling their image' all the time, and that manipulation by others is extremely easy. The Principal/Governors will give consideration to whether the 'image' had been created voluntarily by the member of staff.

- All employees are expected to behave appropriately and responsibly, and should be aware that they may be accountable to the Academy for actions outside of their work.

  This policy clarifies that online conduct is the employee's responsibility, and it is important that staff are aware that posting information on social networking sites cannot be isolated from their working life.

  Any information published online can be accessed around the world within seconds and will be publicly available for all to see, and is not easy to delete/withdraw once published. The Academy views any comment that is made on a social media site as made publicly, and that any inappropriate comment made, will be considered in the context of which it is made. Staff are advised to be mindful that nothing on a social media site is 'private' so comments made must still meet the standards of the Employee Code of Conduct and other relevant policies.

  Staff may be accountable for actions outside of work, including making comments on social media sites, if that is contrary to any of Academy's policies, impacts on or compromises the employee's ability to undertake their role, or undermines management decisions. Such behaviour would be investigated and may result in disciplinary action being taken, and ultimately could result in dismissal.

- Many staff will use social networking outside of work to keep in touch with family, friends or activity groups. For some staff in particular, there may be occasions when contacts within these situations result in links between staff and students at the Academy (for example where there is a pre-existing friendship with the parent of a student). Staff should ensure that in such circumstances they are able to make a professional distinction between their role as a 'friend' outside work and their role within work and clarify their position to such contacts. In such circumstances, staff should declare this to their line manager.

- Whilst generic discussion is not to be discouraged, any communications that employees make through social media must not:

  - bring the Academy into disrepute, for example by:
    - criticising, disagreeing or arguing with parents, colleagues or managers
    - making defamatory comments about individuals or other organisations/groups
    - posting images that are inappropriate or links to inappropriate content

  - breach confidentiality, for example by:
    - referring to confidential information about an individual (such as a colleague or student) or the Academy

  - do anything that could be considered discriminatory against, or bullying or harassment of, any individual or group of individuals, and in contravention of the Academy's policies, for example by:
    - making offensive or derogatory comments relating to sex, gender
    - reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
    - using social media to bully another individual (such as an employee of
    - the organisation)
    - posting images that are discriminatory or offensive or links to such content.

  - take other action that impacts on the employee's ability to do their job, for example by:
    - online activity that is incompatible with the position they hold in the Academy
    - any breach occurring inside or outside the workplace that is likely to affect the employee doing his/her work.

  - contravene the Academy's policies, for example:
    - Staff Code of Conduct, Acceptable Use of IT, the Internet and Electronic Communication, Anti-Bullying Policy, Child Protection/Safeguarding or Single Equalities Policy.

The above examples are not a definitive list of the misuse of social media, but are examples to illustrate what misuse may look like.

- Staff should use common sense when posting items, think about the intended audience and consequences of making unwise remarks about colleagues at the Academy.

- Staff should be aware of the potential risks of communicating with current and ex-students in ways which may be considered as inappropriate – particularly if it could be shown that the adult-student relationship of trust had been breached. The Academy requires staff to only use Academy platforms to communicate with students, in line with the Child Protection/Safeguarding Policy.

  Staff should report any inappropriate contact from students to a member of LT at the earliest opportunity to prevent situations from escalating.

  Staff are reminded that, as a safeguarding issue, they should always be careful about who they are 'talking to'. It is very easy to hide an identity in an on-line conversation.

- Staff are reminded that they have a responsibility to report any racist, sexist or other discriminatory comments they become aware of through postings or chat on such sites.

  Staff are not allowed to access social media sites from the Academy's computers or devices during working hours. Social media sites must not be left 'running' constantly in work's time as this is considered to be a breach of the acceptable use of the internet policy, and would be considered to be using Academy resources for personal use, in work's time, and such would be investigated under the Disciplinary procedure.

- Where the Academy uses official social media channels (such as Twitter and Youtube), the Principal will ensure that there is a reasonable level of monitoring involved to prevent any inappropriate comments, and will ensure students know such monitoring is taking place.

  (See Appendix 4 for further guidance for Principals and staff members)

Safeguarding

- With the increased access of both students and staff to electronic communication, there is an increased chance of a disclosure being made to a member of staff through such a medium. It is increasingly likely that such a disclosure will be made outside normal working hours. Clearly, if the member of staff is not 'logged on' (and there is no expectation that they will be), then they cannot be faulted for taking no action until they receive the message during the next working day. The member of staff will then be expected to follow the normal Academy procedures for reporting a disclosure.

- On receiving a disclosure from a student outside normal Academy working hours, members of staff should contact a senior member of staff, or if unable to do this, ring Call Derbyshire on 01629 533190.

Newly Qualified Staff

There can be particular issues for newly qualified staff relating to the use of social network sites. It is likely that throughout their training period, they will have been regular users of such sites and have possibly been less concerned about the content of their 'pages' or the image they have presented of themselves. As part of their induction, they should be made aware of the issues raised above as a matter of urgency and be advised to remove any material from such sites that may harm their new professional status. As many newly qualified staff may be not much older than some of the students they will be working with, it is extremely important that they are made aware at a very early stage of the potential problems (including loss of job) that inappropriate comments and contact on social network sites (even if outside working hours) can cause.

Devices issued to staff

- The device remains the property of the Academy and is provided to users on a loaned basis. The device provided must not be used by any person(s) other than the authorised user to whom it has been allocated and the property identification tag attached to each device should not be removed for any reason.

- Academy devices have a predetermined list of software installed on the hard drive. No addition or deletion of any software or hardware is permitted without the express permission of the Principal or Network Manager. To ensure that security patches and virus definitions are up to date, staff should connect the device to the Academy network on a regular basis.

- All reasonable care should be taken to prevent loss, damage, theft or unauthorised use of IT equipment as far as is practical. For example, the device should never be left in a vehicle overnight or other unsecured, vulnerable situation. Any loss or damage to Academy IT equipment should be immediately reported to the Principal or Network Manager.

- When a contract of employment at the Academy ends, the employee must return all computer equipment and software to the Network Manager in full working condition. The user account and all personal work stored on the device will then be securely deleted.

- If software/hardware problems arise, the device may need to be restored to its original settings. Work files may be lost during the restoration process, therefore it is the responsibility of all users to ensure that backups of all files are regularly made to an external device, such as the Academy's networked server or encrypted mobile device.

- Where there is evidence that the device has not been used in accordance with the above guidelines, a charge may be made for the replacement or repair of any Academy device whilst on loan.

Health and Safety guidance on using IT equipment including devices

- In the interests of health and safety, staff are advised to adhere to the following recommendations for the safe use of personal devices. Any health and safety concerns associated with the use of devices should be discussed with the Principal.

  - Sit in a chair that provides good back support to avoid backache and position the device directly in front of the user to avoid twisting.
  - Take regular breaks from the screen to reduce eye strain.
  - Avoid using the device on a low table or on the lap as both of these positions will increase strain on the neck and lower back.

  This is not an exhaustive list of advice pertaining to health and safety issues. The HSE publication 'Work with Display Screen Equipment: Health and Safety (Display Screen Equipment) Regulations 1992 as amended by the Health & Safety (Miscellaneous Amendments) Regulations 2002 provides further information and guidance.

Use of other Academy IT Equipment

- Users who borrow equipment from the Academy must sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use. Any loss or damage to equipment on loan should be immediately reported to the Principal or Network Manager in the first instance and any theft or criminal damage should be reported to the Police.

- To prevent data loss and ensure consistent application of Academy policies no personally owned equipment should be attached to the Academy's network without the permission of the Principal or Network Manager. All mobile devices must be encrypted or password protected wherever technology allows.

Software

Users should use software in accordance with applicable licence agreements. To copy software or any supporting documentation protected by copyright is a criminal offence. The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the Academy. Under no circumstances should any user possess unlicensed software on Academy premises or use unlicensed software on Academy IT equipment (including portable equipment).

Network Access, Passwords and Data Security

- Users must only access information held on the Academy's computer systems if properly authorised to do so and the information is needed to carry out their work. Under no circumstances should personal or other confidential information held on the Academy network or IT equipment be disclosed to unauthorised persons. If you accidentally access information, which you are not entitled to view, report this immediately to the Principal or Network Manager.

- All data stored on the Academy servers is backed-up in accordance with the Academy back-up and disaster recovery strategy (appendix 5 attached).

- Staff using computers in classrooms must ensure that sensitive data is not accessible to students or other individuals by logging off or locking the computer. In other areas computers must not be left logged on when unattended.

- Staff passwords must be at least eight characters in length, containing at least one capital letter and one number. Whilst the user account is active the password must be changed on a regular basis, at least termly. System and administration level passwords should also be changed, at least on a termly basis.

- All passwords are to be treated as sensitive, confidential information. Therefore, staff must not:

  - write down passwords or store them on-line.
  - use Academy user account passwords for other types of access (e.g., personal ISP accounts, internet banking, etc.).
  - share passwords with anyone, including line managers, colleagues, administrative assistants or secretaries.
  - reveal a password over the phone or in an e-mail message or other correspondence.
  - talk about a password in front of others including family members.
  - hint at the format of a password (e.g., "my family name").
  - reveal a password on questionnaires or security forms.
  - insert passwords into e-mail messages or other forms of electronic communication.

- If an account or password is suspected to have been compromised, the incident must be reported immediately to the Principal or Network Manager so that the account password can be changed.

Encryption

Sensitive or confidential information held on devices or other portable devices (e.g. memory sticks) should be minimised to reduce risks in case of loss. Encrypted USB sticks should be used if sensitive data is on them.

Monitoring of email

- The Academy reserves the right to make appropriate arrangements to monitor, log record and access all communications at any time without notice. Initially this is done via an electronic system, however if this was triggered by an employee's actions, this would be reported to the Principal. Where there was good cause, this situation would be more closely monitored by the Academy's Network Manager, but only if explicitly requested in writing by the Principal. The Principal will record the reason for the monitoring. Whenever an employee's emails have been accessed/monitored, they will be notified and given the reasons in writing. Other than this employees should be assured that no-one is allowed to read/access their emails.

  The following details are recorded by the system in respect of every email message:

  - name of the person sending the email,
  - the email addresses of all recipients and copy recipients,
  - the size and name of any file attachments,
  - the date and time sent,
  - a copy of the email,
  - a copy of file attachments.

- The Academy may produce monitoring information, which summarises email usage and may lead to further enquiries being undertaken.

  Monitoring information will be kept for six months.

Monitoring Internet Access and Instant Messages

- The Academy logs all internet traffic to protect the Academy and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited.

  The logs record:
  - the network identifier (username) of the user
  - address of the internet site being accessed
  - where access was attempted and blocked by the system

- the web page visited and its content
- the name of any file accessed and/or downloaded
- the identity of the computer on the network and the date and time.

Any excessive or inappropriate use could result in the facility being withdrawn or disciplinary action being taken.

All monitoring information will be kept for six months.

Private Use

- Staff should recognise their responsibility to maintain the privacy of individuals, comply with current legislation and the expectations of the Academy.

- IT resources are provided for Academy business purposes. Reasonable and responsible personal use is allowed, provided there is no conflict with the interests of the Academy. The Academy does not accept liability for any personal loss or damage incurred through using the resources and facilities for private use. The security of private information and data is the responsibility of the user.

- In order to comply with HM Revenue and Customs regulations on taxable benefits any use of a Academy device for an employee's private purposes must not be 'significant'.

Disciplinary and Related Action

- Suspected misuse of the Academy's computer systems by a member of staff will be considered by the Principal. Failure to follow this policy could result in disciplinary action being taken and include warning, suspension, dismissal from Academy and in the case of illegal activities referral to the police.

Summary

- Academy managers have a duty of care to all staff and to ensure that they have a reasonable work-life balance and that they are able to work in a healthy and safe environment. Principals should therefore try to ensure that electronic working does not place greater burdens on staff in terms of either workload or response times. Principals should also endeavour to support any staff who are subject to abuse through any of the electronic media, by effective and immediate sanctions, in the same way with which it is expected verbal and physical abuse would be dealt.

- Staff should always be reminded to think carefully about all forms of communication, but particularly electronic methods (which can be circulated widely and rapidly). If 'thinking about it' gives rise to any doubt, then the best advice is 'do not do it'.

- This is a rapidly changing and developing area. This guidance provides initial advice, of which all staff should be made aware. It is anticipated however that it will be reviewed and updated regularly in the light of technological changes.

Schedule for Review

The implementation of this E-Safety policy will be monitored by the E-Safety Co-ordinator and Leadership Team.

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: July 2018

Should serious E-Safety incidents take place, the following external persons/agencies should be informed: police, social care, LADO.

To be read in conjunction with:

- Child Protection/Safeguarding Policy
- Equality Policy
- Staff Code of Conduct
- Acceptable Use of IT, the Internet and Electronic Communication
- Anti-Bullying Policy

Appendix 1

ELECTRONIC DEVICES - SEARCHING & DELETION

Search:

Students are allowed to bring mobile phones or other personal electronic devices to Academy and use them only within the rules laid down by the Academy. Phones are not allowed out in in lessons or in corridors unless explicit permission is given by the class teacher. If students breach these rules, their phone will be confiscated, kept in a secure, locked place and returned to the student at the end of the Academy day.

Heads of Year, behaviour support and Leadership Team have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the Academy rules.

- Searching with consent - authorised staff may search with the student's consent for any item.
- Searching without consent - authorised staff may only search without the student's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the Academy rules as an item which is banned and may be searched for.

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e. an item banned by the Academy rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student being searched.

The authorised member of staff carrying out the search must be the same gender as the *student* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student* being searched.

There is a limited exception to this rule: authorised staff can carry out a search of a *student* of the opposite gender including without a witness present, but only where it is reasonably believed that there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the student to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags.

A student's possessions can only be searched in the presence of the student and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of force:

Force cannot be used to search without consent for items banned under the Academy rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the Academy rules).

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of Academy discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials.

Care should be taken not to delete material that might be required in a potential criminal investigation.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the Academy rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of Academy discipline) or whether the material is of such seriousness that it requires the involvement of the police. A record should be kept on SIMS of the reasons for the deletion of data / files.

Care of Confiscated Devices

Academy staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices .

Training/Awareness

Members of staff should be made aware of the Academy's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the Academy's E-Safety policy.

Members of staff authorised by the Principal to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Appendix 2

STAFF ACCEPTABLE USE AGREEMENT FOR THE USE OF ACADEMY ICT NETWORK

As a staff user of the Academy network I agree:

- I will only use the Academys email/internet/learning platform and any related technologies for professional purposes or for the uses deemed 'reasonable' by the Chair of the Governing Body.
- I will comply with the ICT security system and not disclose any passwords provided to me by the Academy or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in Academy, taken off the Academy premises or accessed remotely.
- I will not install any hardware or software without permission of the network manager.
- I will not browse, download, upload or distribute any material considered offensive, illegal or discriminatory.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in Academy and outside Academy, will not bring my professional role into disrepute.
- I will support and promote the Academy's E-Safety and data security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I confirm that I have received appropriate training, read and understood the Academy Staff IT Acceptable Use policy on the use of IT resources.

Signature _____ Date _____

Full name _____

Appendix 3

STUDENT ACCEPTABLE USE AGREEMENT FOR THE USE OF THE ACADEMY ICT NETWORK

As a user of the Academy network I agree:

- I will only log on to the Academy network, other resources and the learning platform with my own user name and password.
- I will only use ICT systems in Academy, including the internet, email, digital video and mobile technologies for Academy purposes.
- I will follow the Academys ICT security system and not reveal my passwords to anyone.
- I will make sure that all ICT communications with students, teachers or others are responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidently come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone.
- I will not break copyright law.
- Images of students and/ or staff stored and used for Academy purposes must not be distributed outside the Academy network.
- I will support the Academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Academy community.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, Academy sanctions will be applied and my parent/carer may be contacted.
- I will treat the ICT equipment with care and respect.
- I will not attempt to bypass the Academy's filtering system. I understand that the filtering system is there for my protection and safety.
- I agree to all of the above.

Signature _____ Date _____

Full name _____

Appendix 4

EMPLOYEE GUIDANCE ON THE USE OF SOCIAL MEDIA

- Staff must be mindful that any online activities/comments made in a public domain, must be compatible with their position within the Academy, and safeguard themselves in a professional capacity.
- Protect your own privacy. To ensure that your social network account does not compromise your professional position, ensure that your privacy settings are set correctly. Remember to upgrade access settings whenever the application/programme is upgraded.
- When setting up your profile online consider whether it is appropriate and prudent for you to include a photograph, or provide occupation, employer or work location details. Comments made outside work, within the arena of social media, do not remain private and so can have an effect on or have work-related implications. Therefore, comments made through social media, which you may intend to be "private" may still be in contravention of the Employee Code of Conduct, the Harassment and Bullying Policy and/or the Disciplinary Policy. Once something is online, it can be copied and redistributed making it easy to lose control of. Presume everything you post online will be permanent and can be shared.
- Do not discuss work-related issues online, including conversations about students, parents, complaints, management or disparaging remarks about colleagues or the Academy. Even when anonymised, these are likely to be inappropriate. In addition doing this in the presence of others may be deemed as bullying and/or harassment.
- Do not under any circumstances accept friend requests from a person you believe could be a 'service user' or may conflict with your employment.
- Be aware that other users may access your profile and if they find the information and/or images it contains offensive, make a complaint about you to the Academy as your employer.
- Ensure that any comments and/or images cannot be deemed defamatory, libelous or in breach of copyright legislation.
- You can take action if you find yourself the target of complaints or abuse on social networking sites. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others.
- If you do find inappropriate references and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed. It is wise to alert your friends in advance to the implications for you, as a Academy employee, of posting material related to you.
- If you find inappropriate references to you posted by parents/carers, colleagues, students or other members of the Academy community, report this to the Principal.
- If you are very concerned about someone else's behaviour online, you should take steps to raise your concerns. If these are work related you should inform your manager.
- Staff should also act in accordance with the Academy's Code of Conduct, Acceptable Use of IT, the internet and electronic communication, Child Protection/Safeguarding Policy and Anti-Bullying Policy.
- Staff should not access social media sites or leave these running in the background during working time, on any devices within their control.

Additional Guidance for Principals on the Use of Social Media

Principals have a responsibility to:

- Remain familiar with this policy and the employee guidelines to using social media included in the Appendix.
- Ensure staff are made aware of the policy, employee guidelines and provided with appropriate training/briefing.
- Take prompt action to stop any harassment or bullying they become aware of, whether a complaint has been raised or not, including taking steps to seek the prompt removal of any inappropriate material.
- Make parents and students aware of the implications of posting comments about the Academy and members of its community. Details will be included in the Home Academy Agreement and/or Academy brochure, to indicate the appropriate means for parents of raising any concerns. It is advised that these documents also make reference to the potential implications of posting inappropriate comments about the Academy/staff/students/wider community members. The agreement will also warn against the taking of unauthorised photographs of staff and/or making sound recordings.
- Support employees who are the subject of abuse, through existing policies and procedures.
- Ensure all complaints/allegations are dealt with fairly and consistently, and in accordance with other employment policies where appropriate.

Principals are advised to:

- Ensure staff are advised of this policy on appointment and discussion and elaboration is included during induction such that they are fully aware of its content.
- Remind staff on an annual basis of the guidance on use of social media.
- Ensure staff are aware of how to raise concerns
- Include in the relevant section of the Information and Communication Technology curriculum, advice for students on the safe use of social media, the restrictions on use of these media for contact with Academy staff and the implications of posting material on such sites.
- Provide guidance for parents in supporting their children's safe use of social media
- Include in documents like the Academy brochure and home/Academy agreement the Academy's approach to the taking of photographs of students, by the Academy or by parents, and how these may be used. Seeking parents' agreement at the outset and alerting them to potential pitfalls is likely to reduce issues of concern occurring. Parents may need to be made aware of the potential consequences of posting pictures on social media which include children other than their own, without parents' permission.
- Ensure parents and students are made aware that the use of social media to make inappropriate comments about staff, other parents or students will be addressed by the Academy in the same way as if these remarks were made in person, in the public domain.
- Seek the advice of the local authority if experiencing difficulty in securing the removal of inappropriate material from a site or, in serious cases, for legal advice concerning the content of what has been posted.

Definition of 'libel' and 'defamation'

Any comments or statements made online may be viewed as defamatory/libellous and members of the Academy community need to be aware that they may be also be held accountable for comments made online in a court of law.

Defamation is the act of making a statement about a person or company that is considered to harm their reputation, and may cause actual loss/costs to the person/company. If the defamation is written down (print or online) this is known as libel.

Appendix 5

ICT BACKUP STRATEGY & DISASTER RECOVERY

POLICY STATEMENT

The purpose of this policy is to set in place strategies to ensure the secure backup and recovery of important data that is stored on the Academy administration and curriculum networks. Data requiring backup includes Academy management data files, administration network user documents, teaching staff documents and student documents.

BACKUPS

The following data will be backed up onto backup tapes by the network manager:

Backup Frequency

Network	Data	Backup Frequency	Backup Type
Admin	SIMS Database	Daily	Full/Append
Admin	AD/System State/User areas	Daily	Full/Append
Curriculum	Staff & Student User areas	Weekly	Full
Curriculum	FROG	Weekly	Full
Curriculum	Shared Areas	Weekly	Full
Curriculum	Active Directory/GPO/System State	Weekly	Full
Curriculum Servers	Systems	Quarterly	Full

Physical Location of Backup Tapes

Daily tapes to create a full week's set	Off site - Network Manager
1st Weekly Set	Fireproof safe - Bursar's Office
2nd Weekly Set	Head of ICT - Offsite
3rd Weekly Set	Server Room

As a further precaution against data loss an extra backup of all curriculum network user data is kept on an external hard drive device. This backup is scheduled to run once a week.

As from February 2013 Virtual Servers, which includes the Intranet, will be backed up quarterly onto an external hard drive and when completed will be taken offsite with the Network Manager.

ARCHIVE BACKUPS

The following data will be archived annually onto an external hard drive:

End of Year 11 and Sixth Form (all years)

Website

Hosted externally with 3DPixel who are responsible for its backup.

BACKUP HARDWARE AND SOFTWARE

The network manager will determine the appropriate hardware and software necessary to provide reliable backup and archiving of data on the Academy's network. As the amount of data increases over time the hardware requirements will be reviewed periodically. When adjustments are needed this will be submitted to the Leadership Team.

OLD BACKUP MEDIA

Backup media that is not re-usable will be destroyed thoroughly in an approved manner. Backup media that is used for other purposes will be erased thoroughly.

BACKUP LOGS

The network manager will monitor backup logs to ensure that network data has been fully backed up. Backups will be periodically tested to ensure that data can be correctly restored.

BACKUP OF DATA STORED ON DEVICES\DEPARTMENTAL COMPUTERS

Whilst user data is stored centrally on network servers; individual users are responsible for backing up their own data on staff devices provided by the Academy.

BACKUP SCHEDULES

It is the responsibility of the network manager to provide documentation displaying backup schedules and what is backed up.

DISASTER RECOVERY

Admin network:

To ensure that Academy timetabling, staff cover, financial transactions and any other critical Academy management systems can still run the member of staff responsible for these areas should ensure that they have their own disaster recovery plan. This will then enable them to at least continue working in these areas.

The person responsible for their particular area should follow the following guidelines in formulating their own disaster recovery plan:

- identify essential Academy management functions. Essential Academy functions are those functions that must take place in order to support an acceptable level of continuity for the Academy
- document procedures to implement this disaster recovery plan
- make sure the plan can work effectively in the event of a disaster
- make sure staff that work within these critical Academy management areas are aware of the plan and are able to carry it out effectively
- plan for the alternate processing of data to use during a disaster. This would include keeping hard copies of certain data and documents and documentation of any disaster plan
- make the Leadership Team aware of what strategies would be employed in the event of a disaster.

Curriculum network:

All curriculum backups are a maximum of a week old.

DATA RESTORATION

The network manager will restore curriculum network data when a crisis has occurred after having first consulted with the Head of ICT and/or Leadership Team. The network manager will determine if a successful restoration is possible. (Any requests for restoration of individual user data will be made to the technical team and restoration of user data may occur at the discretion of the network manager).

In the event of complete server failure where a full restoration of Academy management software and data files is necessary, a member of the Leadership Team will need to give approval.