# Madeley Academy


# E-Safety Policy

**Prepared by:** **Ian Marshall**

**Date:** **September 2018**

**Review Date:** **September 2019**

## Contents

Development, monitoring and review of the Policy Schedule for development, monitoring and review Scope of the Policy

| | |
|---|---|
| **Roles and Responsibilities** | Governors<br>Headteacher and Senior Leaders<br>E-Safety Co-ordinator/Officer<br>Network Manager/Technical Staff<br>Teaching and Support Staff<br>Child Protection/Safeguarding Designated Person<br>E-Safety Committee<br>Students<br>Parents/Carers |
| **Policy Statements** | Education – Students<br>Education – Parents/Carers<br>Education and training – Staff/Volunteers<br>Training – Governors<br>Technical – infrastructure/equipment, filtering and monitoring<br>Bring your own devices (BYOD)<br>Use of digital and video images<br>Data protection<br>Communications<br>User Actions – unsuitable/inappropriate activities |
| **Appendices** | Acceptable Use Policy – Staff<br>Acceptable Use Policy – Students<br>Responding to incidents of misuse – flowchart<br>Actions and Sanctions |

## Development, Monitoring & Review of this Policy

This E-Safety Policy has been developed by the E-Safety Working Group:

- D Marshall – Senior Deputy Headteacher in Charge of Safeguarding
- I Marshall - E-Safety Officer
- A Johnson – Coordinator
- S Barnes – Network Manager
- S Maloney – Link governor

## Schedule for Development, Monitoring & Review

| | |
|---|---|
| The implementation of this policy will be monitored by the: | D Marshall - Safeguarding<br>I Marshall – E-Safety Officer<br>A Johnson –E-Safety Co-ordinator<br>S Barnes – Network Manager<br>S Maloney – Link governor |
| Monitoring will take place at regular intervals: | Termly |
| The Governing Board will receive a report on the implementation of the policy generated by the monitoring group (which will include anonymous details of E-Safety incidents) at regular intervals: | Termly |
| 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 each year for publication in September or as developments dictate earlier revision |
| Should serious E-Safety incidents take place, the following external persons/agencies should be informed: | LA Safeguarding Officer, Police |

The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of:
  a) students
  b) parents/carers
  c) staff

## 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.

The Education and Inspections Act 2006 empowers Headteachers 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.

In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The Academy will deal with such incidents 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 the Academy.

## Roles and Responsibilities

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

### Governors: S Maloney

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. **Mrs Sharon Maloney**, a member of the Governing Board has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator and Officer
- regular monitoring of E-Safety incident logs
- regular monitoring of filtering/change control logs
- reporting to Governing Board

### Headteacher and Senior Leaders

The Headteacher 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 Safeguarding Officer, E-Safety Co-ordinator and Officer.

The Headteacher and another member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff (see flow chart on dealing with E-Safety).

The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and Officer 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 Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the Academy who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator and Officer

**E-Safety Coordinator and Officer**

Ian Marshall (E-Safety Officer) has a day to day responsibility for E-Safety. He:

- leads the E-Safety committee
- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the Academy's E-Safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority where appropriate
- liaises with Academy technical staff, receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments,
- meets regularly with E-Safety Governor/Director to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors/Directors
- reports regularly to Senior Leadership Team

Alex Johnson (E-Safety Coordinator) has a day to day responsibility for E-Safety. He

- 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
- liaises with Academy technical staff, receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments (examples of suitable log sheets may be found later in this document)
- meets regularly with E-Safety team to discuss current issues, review incident logs and filtering/change control logs
- ensures E-Safety issues are embedded in all aspects of the curriculum and other activities
- ensures curriculum and staff resources are relevant and up to date.

**Network Manager/Technical Staff**

The Network Manager and IT Technical staff are responsible for ensuring:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack

- that the Academy meets required E-Safety technical requirements and any Local Authority E-Safety policy/guidance which may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that 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
- that the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader/E-Safety Coordinator/Officer for investigation/action/sanction
- that monitoring software/systems are implemented kept up-to-date

**Teaching and Support Staff**

All other 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 Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher/Senior Leader/E-Safety Coordinator/Officer 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
- in lessons where internet use is pre-planned students 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

**Child Protection/Safeguarding Designated Person/Officer**

The Academy Child Protection/Safeguarding Designated Officer is D Marshall (Senior Deputy Head) and is trained in E-Safety issues and 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

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

**E-Safety Group**

The E-Safety Group provides a consultative group that has wide representation from the Academy community, with responsibility for issues regarding E-Safety and the monitoring the E-Safety policy including the impact of initiatives. The group will be responsible for regular reporting to the Governing Body/Directors. Members of the E-Safety Group will assist the E-Safety Coordinator/Officer with:

- The production/review/monitoring of the Academy E-Safety policy/documents
- The production/review/monitoring of the Academy filtering policy and requests for filtering changes
- Mapping and reviewing the E-Safety curricular provision – ensuring relevance, breadth and progression
- Monitoring network/internet/incident logs
- Consulting stakeholders – including parents/carers and the students about the E-Safety provision
- Monitoring improvement actions identified through use of the 360 degree safe self review tool

**Students**

- are responsible for using the Academy digital technology systems in accordance with the Student Acceptable Use Policy
- 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 school and realise that the Academy's E-Safety Policy covers their actions out of school, 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 understand these issues through parents' evenings, newsletters, letters, website and information about national/local E-Safety

campaigns/literature. 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' sections of the website/VLE and on-line student records
- their children's personal devices in the Academy (where this is allowed)

## 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 is broad, relevant and provides 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 Computing/PHSE/other lessons and should be regularly revisited
- Key E-Safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the Academy
- Staff will act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where 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 (eg 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/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 can 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/carers through:

- Curriculum activities
- Letters, newsletters, web site
- High profile events/campaigns eg Safer Internet Day
- Reference to the relevant web sites/publications

**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 should receive E-Safety training as part of their induction programme, ensuring that they fully understand the Academy's E-Safety policy and Acceptable Use Agreements
- The E-Safety Coordinator/Officer 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 in staff/team meetings/INSET days
- The E-Safety Coordinator/Officer will provide advice/guidance/training to individuals as required

**Training – Governors/Directors**

Governors take part in E-Safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/E-Safety/Health & Safety/Child Protection. This will be offered by participation in Academy training/information sessions for staff or parents.

**Technical – Infrastructure/Equipment, Filtering & Monitoring**

The Academy is responsible for ensuring that the Academy's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will ensure that the relevant people named in the previous sections will be effective in carrying out their E-Safety responsibilities

- Academy technical systems will be managed in ways that ensure that the establishment 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 by S Barnes (Network Manager) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The "master/administrator" passwords for the Academy ICT system used by the Network Manager must also be available to the Headteacher or other nominated Senior Leader and kept in a secure place
- S Barnes 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. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.

- The Academy has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/students etc)
- Academy technical staff regularly monitor and record the activity of users on the 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 relevant person
- 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" (eg trainee teachers, supply teachers, visitors) onto the Academy's systems
- An agreed policy is in place regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on the Academy devices that may be used out of the Academy
- An agreed policy is in place that prevents staff from downloading executable files and installing programmes on school devices
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on the Academy devices. Personal data cannot be sent

over the internet or taken off the Academy site unless safely encrypted or otherwise secured

**Bring Your Own Device (BYOD)**

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. However, there are a number of E-Safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The Academy has a set of clear expectations and responsibilities for all users
- The Academy adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the Academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the Academy will follow the process outlined within the BYOD 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 eg on social networking sites

- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images
- 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. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes
- 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

## Communications

| Communication Technologies | Staff & Other Adults | | | | Students | | | |
|---|---|---|---|---|---|---|---|---|
| | **Allowed** | **Allowed at certain times** | **Allowed for selected staff** | **Not allowed** | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to the Academy | ✓ | | | | ✓ | | | |
| Use of mobile phones in lessons | | ✓ | | | | ✓ | | |
| Use of mobile phones in social time | ✓ | | | | | ✓ | | |
| Taking photos on mobile phones/cameras | | ✓ | | | | | ✓ | |
| Use of other mobile devices eg tablets, gaming devices | | | | × | | | ✓ | |
| Use of personal email addresses in the Academy, or on the Academy network | | | | × | | | | × |
| Use of the Academy email for personal emails | | | | × | | | | × |
| Use of messaging apps | | ✓ | | | | | | × |
| Use of social media | | | | × | | | | × |
| Use of blogs | | | | × | | | | × |

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

- The official Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students will therefore use only the Academy email service to communicate with others when in the Academy, or on Academy systems (eg by remote access)
- Users must immediately report, to the nominated person – in accordance with the Academy policy, the receipt of 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, 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 social media must not be used for these communications
- 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

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Un-acceptable | Un-acceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | pornography | | | | X | |
| | promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute | | | | X | |

| | | | | | |
|---|---|---|---|---|---|
| Using Academy systems to run a private business | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Academy | | | | X | |
| Infringing copyright | | | | X | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | X | |
| On-line gaming (educational) | | X | | | |
| On-line gaming (non educational) | | X | | | |
| On-line gambling | | | | X | |
| On-line shopping / commerce | | | X | | |
| File sharing | | X | | | |
| Use of social media | | X | | | |
| Use of messaging apps | | | X | | |
| Use of video broadcasting eg Youtube | | X | | | |

# Appendices

## Staff - Acceptable Use Policy Agreement

*The aim of this policy is to provide clarification to staff on the use of emerging technologies so that a teacher's professional position is not compromised. It should be read in conjunction with the Child Protection Policy which offers further guidance on safeguarding issues.*

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 students 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 young people.

For my professional and personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of the Academy ICT systems (eg laptops, email, VLE etc) out of the Academy, and to the transfer of personal data (digital or paper based) out of the Academy
- I understand that the Academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person
- I will not communicate with students through social networking sites such as Facebook or on Twitter. I will not under any circumstances accept friend requests from a person who I believe to be either a parent/carer or a student at the Academy. I am responsible for ensuring that privacy settings are enabled and that private content is not available to students. If I require support with this the IT staff will help me
- I will not issue my mobile phone number to students or ask for students' mobile phone numbers or keep a record of student mobile phone numbers for reasons other than official Academy business eg speaking to parents

I will be professional in my communications and actions when using 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 my personal equipment to record these images, unless I have permission to do so.
- I will not use chat and social networking sites in the Academy in accordance with the Academy Policy
- I will only communicate with students and parents/carers using official Academy systems. Any such communication will be professional in tone and manner and any protracted communication will be referred to my line manager
- I will not engage in any on-line activity that may compromise my professional responsibilities

The Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy:

- When I use my mobile 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 Academy 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 hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will not try (unless I have permission) to 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 programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in Academy policies
- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage
- I understand that data protection policy requires that any staff or student 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 Academy 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 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 Academy ICT equipment in the Academy, but also applies to my use of Academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the Academy's 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 Name (Print) | |
| Signed | |
| Date | |

## Student - Acceptable Use Policy Agreement

I understand that I must use 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.

For my own personal safety:

- I understand that the Academy will monitor my use of the systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger", when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc )
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Academy systems and devices are intended for educational use and that I will not use them for personal or recreational use
- I will not try to 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 use the Academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube)

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not take or distribute images of anyone without their permission

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure its smooth running:

- I will only use my own personal devices (mobile phones/USB devices etc) in the Academy if I have permission. I understand that, if I do use my own devices in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programs of any type on any Academy device, nor will I try to alter computer settings
- I will not use social media sites

When using the internet, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me

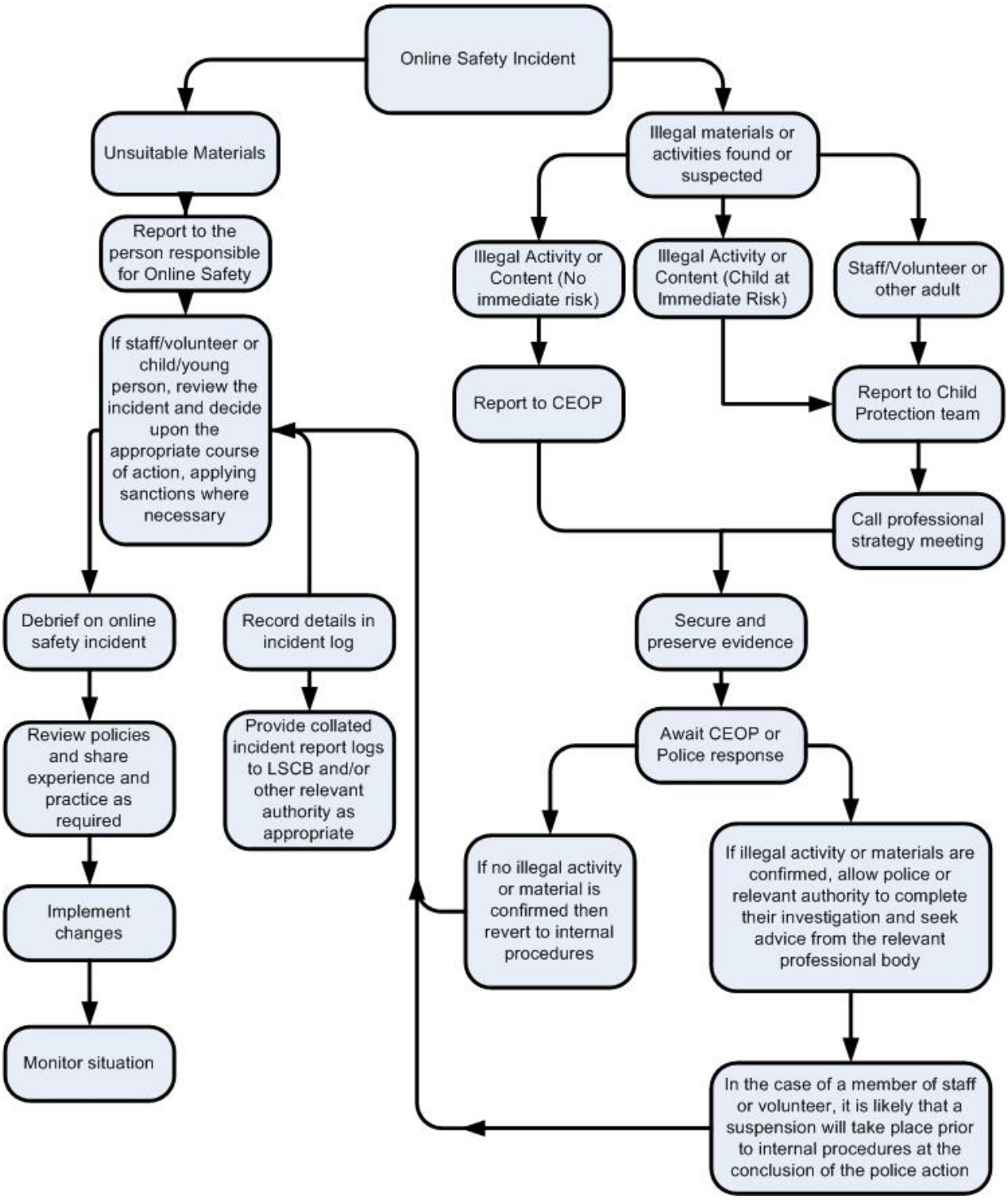
I understand that I am responsible for my actions, both in and out of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

| | | | |
|---|---|---|---|
| Name (Print) | | Year Group | |
| Signed | | | |
| Date | | | |

## 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 (below and appendix) for responding to online safety incidents and report immediately to the police.



## Other Incidents

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

Have more than one senior member of staff/volunteer 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)

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 (as relevant)
- 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. The completed form should be retained by the group for evidence and reference purposes.

## Academy Actions & Sanctions

**Students** **Actions / Sanctions**

| Incidents: | Refer to class teacher / tutor | Refer to Head of Department / Head of Year / other | Refer to Headteacher / Principal | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
|---|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities) | X | | X | X | X | X | X | X | X |
| Unauthorised use of non-educational sites during lessons | X | | | | X | X | X | X | X |
| Unauthorised use of mobile phone/digital camera other mobile device | X | X | | | | | | | X |
| Unauthorised use of social media/ messaging apps/personal email | X | X | | | X | | X | X | X |
| Unauthorised downloading or uploading of files | X | X | | | X | | X | X | X |
| Allowing others to access Academy network by sharing username and passwords | | | | | X | | X | X | X |
| Attempting to access or accessing the Academy network, using another student's account | | | | | X | | | X | X |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Attempting to access or accessing the Academy network, using the account of a member of staff | X | X | | | X | X | | X | X |
| Corrupting or destroying the data of other users | X | X | | | X | | X | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | X | X | X | X | X | X |
| Continued infringements of the above, following previous warnings or sanctions | X | X | | | X | | X | | X |
| Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy | | | | | X | X | X | X | X |
| Using proxy sites or other means to subvert the Academy's filtering system | X | X | | | X | | X | X | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | | | | | | | X | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | | | X | | X | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | | | | | | | X | |

| Staff | Actions / Sanctions | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Incidents: | Refer to line managerr | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities) | | X | X | X | X | X | X | X |
| Inappropriate personal use of the internet/social media personal email | X | | | | X | X | | |
| Unauthorised downloading or uploading of files | X | | | | X | X | | |
| Allowing others to access the Academy's network by sharing username and passwords or attempting to access or accessing the Academy's network, using another person's account | | | | | X | X | | |
| Careless use of personal data eg holding or transferring data in an insecure manner | X | | | | X | X | | |
| Deliberate actions to breach data protection or network security rules | X | | | | X | X | | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | | | X | X | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | | X | X | X | X | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students | X | | | | X | X | | |
| Actions which could compromise the staff member's professional standing | X | | | | X | X | | |
| Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy | X | X | | | X | X | | |
| Using proxy sites or other means to subvert the Academy's filtering system | X | | | | X | X | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | | | | X | X | | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | | X | X | X | | X |
| Breaching copyright or licensing regulations | X | | | | X | X | | |
| Continued infringements of the above, following previous warnings or sanctions | X | X | | | X | X | X | X |