Windsor Academy Trust

E-Safety Policy	
Responsible Committee:	Windsor Academy Trust, Board of Directors
Date revised by Board of Directors:	December 2016
Next review date:	December 2017

1. **Scope of the Policy**

This policy applies to all members of the WAT community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of the Trust's IT systems..

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 academy 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.

2. Roles and Responsibilities

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

2.1 Board of Directors:

- Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of this policy and its appropriate implementation.

2.2 Chief Executive (CEO) and Headteachers / Academy Leadership Teams:

- The CEO and WAT Leadership Teams have a duty of care for ensuring the safety (including E-Safety) of members of the WAT community; the day to day responsibility for E-Safety will be delegated to the Trust and Academy's E-Safety Co-ordinators.
- The CEO and WAT Leadership Teams 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 CEO and WAT Leadership Teams are responsible for ensuring that the 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 CEO and WAT Leadership Teams will ensure that there are systems in place to allow for monitoring and support of those in WAT 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 CEO/Leadership Teams will meet with their respective E-Safety Co-ordinators, receive regular monitoring reports of E-Safety incident logs and filtering / change control logs

2.3 Trust / Academy E-Safety Coordinators:

- The Trust E-Safety Coordinator leads and coordinates the team of Academy E-Safety Coordinators
- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the Trust E-Safety policies
- 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
- Reports regularly to the Executive and Leadership Teams on current issues, reviews incident logs and filtering / change control logs

2.4 IT Infrastructure / Technical staff:

The IT Infrastructure Lead is responsible for ensuring:

- That the Trust's technical infrastructure is secure and is not open to misuse or malicious attack
- That the Trust meets required any E-Safety Policy / Guidance that 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 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 (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the CEO, Headteacher / Leadership Team; E-Safety Coordinator for investigation / action / sanction
- That monitoring systems are implemented and updated as agreed in academy policies.

2.5 Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current academy E-Safety policy and practices
- They have read, understood and signed the staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Headteacher / Leadership Team; E-Safety Coordinator 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.
-

2.6 Child Protection / Safeguarding Designated Person:

Should be trained in E-Safety issues and be 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.

2.7 E-Safety Group:

The E-Safety Group provides a consultative group that has wide representation from the WAT community, with responsibility for issues regarding E-Safety and the monitoring the E-Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Directors.

Members of the E-Safety Group will assist the E-Safety Coordinator with:

- The production / review / monitoring of the 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 SWGfL 360 degree safe self-review tool.

2.8 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 the academy and realise that the Trust's E-Safety Policy

covers their actions out of the academy, if related to their membership of the academy.

2.9 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 Trust will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local E-Safety campaigns / literature. Parents and carers will be encouraged to support the Trust/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).

3. Policy Statements

3.1 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access online 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
- Students should be helped to understand the need for the Student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside academy
- Staff should 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 should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where 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 and 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.

3.2 Education – Parents / Carers:

Parents and carers may have 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 online 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:

- Curriculum activities
- Letters, newsletters, website, VLE
- Parents / carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

3.3 Education – The Wider Community:

The trust will provide opportunities for local community groups / members of the community to gain from the academy's E-Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and E-Safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide E-Safety information for the wider community
- Supporting community groups e.g. early years settings, child-minders, youth / sports / voluntary groups to enhance their E-Safety provision.

3.4 Education & Training – Staff / Volunteers:

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 Trust E-Safety policy and Acceptable Use Policies.
- The E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from LA / other relevant organisations) 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 will provide advice / guidance / training to individuals as required.

3.5 Training – Directors:

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in Academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

3.6 Technical – infrastructure / equipment, filtering and monitoring:

The Trust will be responsible for ensuring that the trust's infrastructures / networks are safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-Safety responsibilities:

- The Trust's technical systems will be managed in ways that ensure that the academies meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academies 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 from the IT Technical Support team. Users are responsible for the security of their username and password and will be required to change their password every 6 months
- The " administrator" passwords for the academy IT systems, used by the Network Manager (or other person) must also be available to the Headteacher (Academy Headteachers) or other nominated senior leader and kept in a secure place
- The IT Technical Team are 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. (There is a clear process in place to deal with requests for filtering changes)
- The IT Technical Team has provided enhanced / differentiated user-level filtering
- IT 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 Policy (Agreement).

- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and mobile devices for example, 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, visitors) onto the academy 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 trust devices that may be used outside of the academy.
- An agreed policy is in place that forbids staff from downloading executable files and installing programs on academy devices (Guardianship Agreement)
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on academy devices. Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured (AUP).

4. **Bring Your Own Devices (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. This has led to the exploration by academies of users bringing their own technologies in order to provide a greater freedom of choice and usability. 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.

- 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 Policy (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
- Users can 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
- 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.

5. **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 cyber bullying 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 (see Social Media Policy).
- 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 everyone's 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.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the academy website
- Student's work can only be published with the permission of the student and parents or carers.

6. **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 trust ensures that:

- It shall hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- 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 has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- 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
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

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

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

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with academy policy (below) once it has been transferred or its use is complete (see AUP)

7. **Communications:**

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

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

- The official trust email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the trust email service to communicate with others when in the academy, or on academy systems (e.g. 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, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) trust 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 trust or its academy websites and only official email addresses should be used to identify members of staff.

8. **Social Media - Protecting Professional Identity:**

With an increase in use of all types of social media for professional and personal purposes the policy sets out clear guidance for staff to manage risk and behaviour online. Core messages include the protection of students, the academy and the individual when publishing any material online. Refer to the WAT Social Media Policy.

9. **Unsuitable / Inappropriate Activities:**

The trust believes that the activities referred to in the following section would be inappropriate in a trust context and that users, as defined below, should not engage in these activities inside or outside of the trust's buildings when using trust equipment or systems.

10. **Radicalisation and Extremism**

Prevent (2015) Training is an integral part of our Safeguarding policy and training for all staff. We know that students may actively search online, and may be persuaded to by others or may come across material that is considered radical. A number of social media sites can be, and have been used by extremists trying to identify, target and contact students. Not everyone online is who they say they are which can sometimes deceive students into believing they are talking to someone who they do not really know. These people can try to encourage students to consider or embrace extreme views and beliefs. To prevent the latter, and as part of our safeguarding responsibility we have a

monitoring tool (Impero) in place that can help alert us to items deemed to be indicators of vulnerability to radicalisation and extremism.

11. Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

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 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 (e.g. www.xxxx.com) 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 appropriate documentation (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 (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 documentation should be retained by the group for evidence and reference purposes.

12. Trust Actions and Sanctions

It is more likely that the trust 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 trust are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.