Windsor Academy Trust
(The Kingswinford School)

E-Safety Policy	
Responsible Committee:	Windsor Academy Trust, Board of Directors
Date revised by Board of Directors:	January 2019
Next review date:	January 2021

1. Introduction

1.1 Windsor Academy Trust (WAT) has outlined its commitment to safeguarding and promoting the welfare of all pupils/students in its Childs Protection and Safeguarding and Health and Safety Policies. Safeguarding determines the actions taken to keep children safe and protect them from harm in all aspects of their school life to ensure that they have the best outcomes. This is underpinned by a culture of openness where both children and adults feel secure, able to talk, and believe that they are being listened to.

1.2 WAT has also developed a Social Media Policy which should also be referred to alongside this policy as this policy provides more details about the use of social media by staff, volunteers, trustees, pupils/students and parents/carers.

1.3 **Windsor Academy Trust is committed to:** fulfilling its moral and statutory responsibility, ensuring that robust procedures are in place, outlining the actions that it will take to prevent harm, to promote well-being, to create safe environments and to respond to specific issues and vulnerabilities.

1.4 WAT will meet its commitment by:

- Having robust processes in place to ensure the online safety of pupils/students, staff, volunteers, trustees and governors.
- Delivering an effective approach to online safety, which empowers WAT to protect and educate the whole WAT community in its use of technology
- Establishing clear mechanisms to identify intervene and escalate an incident, where appropriate.

2. Purpose

2.1 The purpose of this policy is to safeguard pupils/students, staff, volunteers, governors and trustees from the many issues that can arise as a result of using electronic media.

3. Compliance with Legislation and Guidance

3.1 This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

3.2 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils'/students' electronic devices where they believe there is a 'good reason' to do so.

3.3 The policy also takes into account the National Curriculum computing programmes of study.

4.   Compliance with related policies and agreements

4.1   This policy complies with WAT's funding agreement and Articles of Association.

4.2   This online safety policy is also linked to the following WAT policies:

- Child Protection and Safeguarding
- Health and Safety
- Data Protection
- Information Security and Acceptable Use
- Behaviour (Code of Conduct)
- Social Media
- Disciplinary
- Data Protection and privacy notices
- Complaints Policy

4.3   It should also be read in conjunction with academy pupil/student behaviour policies and procedures.

5.   Governance

Board of Directors

5.1   The Board of Directors (BoD) has overall responsibility for monitoring this policy and for holding the WAT Executive Team and Headteachers to account for its implementation. WAT has a designated Director who oversees the governance arrangements for safeguarding and liaises with the Local Advisory Bodies (LABs) Designated Safeguarding Governors (DSG). The governance arrangements are outlined further in WAT's Child Protection and Safeguarding and also reference to the WAT Health and Safety Policies which should also be referred to in conjunction with this policy.

Local Advisory Bodies

5.2   The Local Advisory Bodies (LABs) will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Leads (DSLs) as part of their responsibilities for Child Protection and Safeguarding.

 5.3   All LAB members will:

- Ensure that they have read and understand this policy.

- Agree and adhere to the terms on acceptable use of WAT's ICT systems and the internet (appendix 2).

- Discharge their responsibilities outlined in the Scheme of Delegation and LAB Terms of Reference.

The Headteacher

5.4   The headteacher is accountable to the Chief Executive and the BoD and is responsible for ensuring that staff understand this policy, and for its consistent and effective implementation in their academy.

The Designated Safeguarding Lead (DSL)

5.5   The details and roles of each academy's DSL are set out in WAT's Child Protection and Safeguarding Policy.

5.6   The DSLs have lead responsibility for online safety, in particular:

- Supporting the headteacher in ensuring that staff and volunteers understand this policy and that it is being implemented consistently throughout the academy and across WAT.

- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy's behaviour policy.

- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs.)

- Liaising with other agencies and/or external services if necessary.

- Providing regular reports on online safety in academies to the headteacher and/or Local Advisory Bodies.

5.7   This list is not intended to be exhaustive.

The ICT Manager

5.8   The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students/pupils and staff safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

- Ensuring that ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

- Conducting a full security check and monitoring WAT ICT systems on a regular basis.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's behaviour policy.

5.9   This list is not intended to be exhaustive.

Trustees, LAB member, staff, and volunteers

5.10   All staff, including contractors, agency staff, volunteers, trustees and LAB members are responsible for:

- Maintaining an understanding of this policy.

- Implementing this policy consistently.

- Agreeing and adhering to the terms on acceptable use of WAT's ICT systems and the internet (Appendix 2) and in accordance with WAT's Information Security and Acceptable Use Policy, and for ensuring that pupils/students follow the terms on acceptable use (Appendix 1).

- Working with the DSLs to ensure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's behaviour policy.

5.11   This list is not intended to be exhaustive.

Parents/Carers

5.12   Parents/Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

- Ensure their child has read, understood and agreed to the terms on acceptable use of the ICT systems and internet (Appendix 1).

5.13   Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

5.14   Visitors and members of the community who use WAT's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

6.   Educating pupils/students about online safety

6.1   The safe use of social media and the internet will also be covered in relevant subjects and the academy will raise pupils'/students' awareness of the dangers that can be encountered online and may, for example, invite speakers to talk to pupils/students about this.

6.2   Pupils/students will be taught about online safety as part of the curriculum.

6.3   In **Key Stage 3**, students will be taught how to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.

- Recognise inappropriate content, contact and conduct, and know how to report concerns.

6.4   Students in **Key Stage 4** will be taught how to:

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity.

- Report a range of concerns.

6.5   Students in **Key Stage 5** will be taught how to:

- Live safely in an online and connected world protecting their privacy; protecting their 'online presence'

- Appreciate how social media can expand, limit or distort their view of the world.

- Set and maintain clear boundaries around their personal privacy; protect their online privacy and identity.

7.   Educating parents/carers about online safety

7.1   WAT will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via WAT websites or any virtual learning environment (VLE) and this policy will also be made available to parents/carers.

7.2   If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

7.3   Concerns or queries about this policy can be raised with any member of staff or the headteacher.

8.   Cyber-bullying

8.1   Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

8.2   To help prevent cyber-bullying, WAT will ensure that pupils/students understand what it is and what to do if they become aware of it happening to them or others. WAT will ensure

that pupil/students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

8.3   The academy will actively discuss cyber-bullying with pupils/students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

8.4   Tutor group/ class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

8.5   Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

8.6   All staff, governors, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils/students, as part of safeguarding training.

8.7   The academy also provides information/leaflets on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

8.8   In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy's behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils/students, the academy will use all reasonable endeavours to ensure the incident is contained.

8.9   The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so. They may liaise with the WAT DSL if appropriate to do so.

9.   **Examining electronic devices**

9.1   WAT staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils'/students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

9.2   When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

9.3   If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- Report it to the police.

9.4   Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

9.5   Any complaints about searching for or deleting inappropriate images or files on pupils'/students' electronic devices will be dealt with through the WAT's Complaints Policy.

10.   Acceptable use of ICT systems

10.1   All pupils/students, parents/carers, staff, volunteers, trustees and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

10.2   Use of WAT's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

10.3   WAT will monitor the websites visited by pupils/students, staff, volunteers, trustees, governors and visitors (where relevant) to ensure they comply with the above.

10.4   More information is set out in the acceptable use agreements in Appendices 1 and 2.

11   Pupils/students using mobile devices in school

11.1   In academies where mobile devices are allowed to be brought into school. Pupils/students are only permitted to use these during breaks unless authorised to do so by a member of teaching staff or at any other time or situation identified within the academy's Behaviour Policy. They are not permitted to use them during:

- Lessons

- Tutor group time

- Clubs before or after school, or any other activities organised by the school

11.2   Any use of mobile devices by pupils/students must be in line with the acceptable use agreement (see Appendix 1).

11.3   Any breach of the acceptable use agreement by a pupil/student may trigger disciplinary action in line with the academy's behaviour policy, which may result in the confiscation of their device.

11.4   Where a pupil/student misuses the ICT systems or internet provided by WAT, WAT will take action as outlined in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

12. Staff using work devices outside of WAT

12.1 Staff members using a work device outside of WAT must not install any unauthorised software on the device and must not use the device in any way which would violate the terms of acceptable use, as set out in the WAT Information Security and Acceptable Use Policy and Appendix 2 of this policy.

12.2 Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of WAT.

12.3 If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

12.4 Where a staff member misuses WAT's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with WAT's Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

12.6 WAT will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

13.1 The DSLs will complete regular child protection and safeguarding training as outlined in the WAT Child Protection and Safeguarding Policy. The training will also include online safety, at least every 2 years. The DSLs will update their knowledge and skills on the subject of online safety at regular intervals, and at least annually and will ensure that all staff are trained and up to date with policies and procedures.

13.2 WAT will be assured that each academy comply with training requirements as defined in KCSIE 2018. All staff will undergo safeguarding and child protection training at induction on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

13.3 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

13.4 Directors/trustees and LAB members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

13.5 Volunteers will receive appropriate training and updates, if applicable.

14. Monitoring arrangements

14.1 The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

14.2 This policy will be e reviewed and agreed as a minimum on a biannual basis and in conjunction with the Child Protection and Safeguarding Policy. This may be more frequent if national guidance requires ensuring that key statutory requirements are incorporated.

Acceptable Use Agreement (pupils/students and parents/carers)

.Acceptable use of the ICT systems and internet provided by Windsor Academy Trust (WAT)

Name of pupil/student:

When using WAT ICT systems and accessing the internet in the academy or on any other WAT premises I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the academy's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into the academy:
- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I understand that the trust will monitor the websites I visit.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
I will always use the ICT systems and internet responsibly.

Signed (pupil/student):	**Date:**

Parent/carer agreement: I agree that my child can use the ICT systems and internet provided by Windsor Academy Trust (WAT) when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the WAT ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Acceptable Use Agreement (trustees, LAB, staff, volunteers, trustees, and visitors)

Acceptable use of the ICT systems and internet provided by Windsor Academy Trust (WAT)
Name of trustee, LAB member, staff/volunteer/visitor:
When using ICT systems provided by Windsor Academy Trust (WAT)and accessing the internet on WAT premises or using WAT devices, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the reputation of the trust • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the WAT network using someone else's details
I will only use WAT ICT systems and access the internet on WAT premises or outside on a WAT device, for educational purposes or for the purpose of fulfilling the duties of my role. I understand that WAT will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and WAT Data Protection Policies including the Information Security and Acceptable Use Policy. I will let the Designated Safeguarding Lead (DSL) and ICT manager know if a pupil/student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use WAT's ICT systems and internet responsibly, and ensure that pupils/students in my care do so too.

Signed (trustee, LAB member, staff/volunteer/visitor):	**Date:**

Online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in your academy?	
Do you know what you must do if a pupil/student approaches you with a concern or issue?	
Are you familiar with the WAT acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils/students and parents/carers?	
Do you regularly change your password for accessing the WAT ICT systems?	
Are you familiar with WAT's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Online Safety Incident Report Log

(*To be completed if information not captured on electronic recording system*)

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**