Washwood Heath
Multi Academy Trust

E-Safety Policy

Prepared by:	Russell Kennedy (Interim Safeguarding Lead)
Applies to:	Employees and Pupils at WHMAT Academies
Approved by:	Board of Trustees on 17.10.19
Issued to WHMAT Academies for use:	TBC
Annual review date:	12 months from ratification by Board of Trustees
Links to:	WHMAT Social Media Policy Local Academy Behaviour Policies WHMAT Safeguarding Policy WHMAT Disciplinary Policy & Procedure WHMAT Code of Conduct WHMAT GDPR Data Protection Policy
Version:	01.10.2019

CONTENTS

1. Introduction

1.1 The Board of Trustees of Washwood Heath Multi Academy Trust ("WHMAT") have adopted this policy to help WHMAT to meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

2. Policy Scope

2.1 This policy refers to the on-site internet connection at each WHMAT site and WHMAT provided ICT devices, systems, and peripherals. These include but are not limited to:

- Fixed computers in offices and classrooms;
- WHMAT provided laptops, tablets and phones;
- WHMAT email systems;
- Remote access solutions to WHMAT networks;
- WHMAT digital cameras, camcorders and audio recorders.

This policy explains the behaviours, which are acceptable and unacceptable with regard to usage of ICT.

2.2 All users should note that ICT systems and internet usage are monitored on a regular basis. Any user who is found to deliberately infringe this policy may be subject to disciplinary procedures or legal action.

2.3 This policy also refers to staff's personal use of the internet (on and off-site) though social media and other forms of internet communication, including the use of personal mobile devices.

2.4 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. 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' electronic devices where they believe there is a 'good reason' to do so.

3. Unlawful and Illegal Use

3.1 All material, which depicts the abuse of children and young people, is illegal.
Other illegal material includes race hatred and incitement to violence. These are not exclusive categories.

3.2 There may be other information that is deemed to be illegal.

3.3 Accidental access to material, which may be classed as illegal should be reported to the Internet Watch Foundation – www.iwf.org.uk as well as directly to the Head of Academy (Head of School in the case of Tile Cross and/or Saltley Academies].

3.4 **If you receive images or content including sound files, which you believe could be illegal it is imperative that you make no attempt to investigate the content.** A written signed and dated log of the incident should be made to show that there is suspicion of inappropriate or illegal material. This log is to protect you from any suspicion for having potential illegal material in your possession. This log should then be submitted to the Head of School. Once this log has been made the URL if appropriate should be reported to the Internet Watch Foundation – www.iwf.org.uk. This must be done by typing the URL address into the report not by copy and paste. It is possible to accidentally open a link so care must be taken.

3.5 If the content is an image in the body of an email close the email and make a log of the incident as above. A report should be made to the IWF. They will advise what to do next. **Under no circumstances forward the email, copy the image or show it to another person, as each of these actions constitutes an illegal offence.** The IWF, is licensed to investigate, you are not. For guidance in this area refer to a member of the Senior Leadership team.

3.6 As a user of ICT within the WHMAT you agree not to use the ICT facilities to create, send, or receive materials or data, which are:

- in violation of any law or regulation;
- which is defamatory, offensive, abusive, indecent, obscene;
- which constitutes harassment;
- in breach of confidence, privacy, trade secrets;
- in breach of any third party Intellectual Property rights (including copyright);
- in breach of any other rights or has any fraudulent purpose of effect.

3.7 You are prohibited from storing, distributing, transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of, any unlawful material through academy systems.

4. Basic principles

4.1 In adopting this policy the directors have taken into account the expectation by Ofsted that rigorous e-safety policies and procedures are in place within WHMAT, written in plain English, with contributions from the whole trust, updated regularly and ratified by the Board of Trustees.

4.2 The policy applies to all members of the WHMAT community, including staff, pupils, volunteers, parents, carers, directors, governors, visitors and community users who have access to, and are users of, WHMAT's information and communication technology systems or who use their personal devices in relation to their work at WHMAT.

4.3 The directors expect the heads of academy to ensure that this policy is implemented, that training in e-safety is given high priority across the academies, that consultations on the

details of the arrangements for e-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to the directors for approval.

4.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the procedure for safeguarding children approved by the Birmingham Safeguarding Children Board. It will also be applied in conjunction with the academy's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

4.5 The directors expect the heads of academy to arrange for this policy to be published to all employees and volunteers in the academy and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

5. Roles and responsibilities

Board of Trustees

5.1 The Board will consider and ratify this policy, in line with recommendations from relevant head office directors. Directors/governors are expected to follow the policy in the same way as volunteers are expected to follow it, including participating in e-safety training if they use information and communication technology in their capacity as academy directors/governors.

5.2 Directors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head of Academy

5.3 The Head of Academy at each WHMAT site is responsible for ensuring that:

- the directors are offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other academy policies, including that on pupils' behaviour, take account of this e-safety policy;
- the directors are given necessary advice on securing appropriate information and communication technology systems;
- the academy obtains and follows City Council or other reputable guidance on information and communication technology to support this policy;
- the academy has a designated senior person to co-ordinate e-safety and that this person has adequate support from, and provides support to, other employees, particularly the designated senior person for safeguarding;
- there is effective consultation with all employees, and other users of the academy's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
- the academy provides all employees with training in e-safety relevant to their roles and responsibilities and that training is also provided to volunteers and directors/governors who use information and communication technology in their capacity as volunteers or directors/ governors, as the case may be;
- pupils are taught e-safety as an essential part of the curriculum;

- the senior leadership team is aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem ;
- records are kept of all e-safety incidents and that these are reported to the senior leadership team;
- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the academy's information and communication technology systems;
- there is appropriate supervision of, and support for, technical staff;
- any outside contractor which manages information technology for the academy undertakes all the safety measures which would otherwise be the responsibility of the academy to the standard required by the academy and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Designated Safeguarding Lead

5.4 Details of each academy's designated safeguarding lead (DSL) and deputies are set out in their Safeguarding and Child Protection policy.

The DSL at each school takes lead responsibility for online safety, in particular:

- Supporting the Heads of School in ensuring that staff understand this policy and that it is being implemented consistently
- Working with the Head of School, ICT manager/technicians and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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 school's Behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety as and when requested.

This list is not intended to be exhaustive.

ICT Technical Support Staff

5.5 The technical support staff is responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus/anti-malware is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly and if required, escalated to Wave 9 as the Trusts' ISP (Internet Service Provider).
- Passwords are applied correctly to all users – the enforced criteria is 8 characters or more, one number and optionally one symbol or more. This in turn will automatically replicate with the O365 and G Suite services, keeping an individual's single password aligned on the new system going forward.
- Personnel/older students are forced to change their password every 200 days.
- The IT System Administrator password is to be changed on a monthly (30 day)

Basis.

Other employees

5.6 Other employees are responsible for

- undertaking such responsibilities as have been delegated by the head of academy commensurate with their salary grade and job descriptions;
- participating in training in e-safety provided by the academy and in consultation about this policy and about its application, including e-safety within the curriculum;
- using information and communication technology in accordance with this policy and the training provided;
- reporting any suspected misuse or problem to the person designated by the academy for this purpose.

Pupils

5.7 Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the academy's behaviour policy and the instructions given to them by staff.

Other users

5.8 Volunteers, including directors/governors, who help in the academy and who use information and communication technology systems and devices in helping the academy are expected to

- participate in training in e-safety provided by the academy in consultations about this policy and about its application, including e-safety within the curriculum;
- use information and communication technology in accordance with this policy and the training provided;
- report any suspected misuse or problem to the person designated by the academy for this purpose.

Parents

5.9 Parents who help in the academy as volunteers are covered by 3.6 above. Parents who are not volunteers in the academy are nonetheless subject to the law in the event of misuse of information and communication technology.

6. Acceptable use

6.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the academy premises.
- The academy's information and communication technology systems are intended primarily for educational use and the management and administration of the academy. During work breaks appropriate, reasonable personal use is permitted.

- General Data Protection regulations and associated legislation must be followed (see WHMAT's GDPR Data Protection Policy at www.washwoodmat.com, policies tab).
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the academy.

6.2 Employees, volunteers, directors and governors should:

- not open, copy, remove or alter any other user's files without that person's express permission;
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- as far as possible communicate with pupils and parents only through the academy's official communication systems and not publish personal contact details through those systems;
- if they occupy a senior post in which they need to keep e-mail and other messages confidential, ask the academy for a separate e-mail address for this purpose;
- if they use personal devices during their work (subject to the agreement of the academy in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- not use personal social networking sites through the academy's information and communication technology systems;
- not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
- ensure that their data is backed-up regularly in accordance with the rules of the academy's systems;
- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the academy's systems;
- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the academy's information and communication technology systems;
- not deliberately disable or damage any information and communication technology equipment;
- report any damage or faults to the appropriate member of staff.

6.3 Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the academy would expect for behaviour and conduct generally (as set out in the trust's code of conduct for support staff and the Teachers' Standards for teachers). The trust accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract or that the trust/academy is, or will be, brought into disrepute.

Social Networking

Staff should refer specifically to the WHMAT Social Media Policy for guidance. The guidance includes but is not limited to:

- Staff members must not have any contact with pupils through personal social media channels, unless the pupils are close friends or family members outside of work. This is because this may constitute a conflict of interest or call into question their objectivity.
- It is not acceptable for staff to make inappropriate comments about their work-place or colleagues on any social media or blog facility
- It is not acceptable for staff to use any social networking sites including (but not limited to) Facebook, Twitter, Snapchat or Instagram, or to blog during working hours
- It is not acceptable for staff or students to make inappropriate comments about the establishment staff or student body on a social network website, or place photographs of them on such sites without permission. Any incidents of this nature should be reported to the leadership team
- Staff are advised to frequently check their privacy settings on social networking sites to ensure they can control who can see the information shared about them, taking care regarding the type of information they publish about themselves or personal photographs. All staff must recognise that there is no such thing as private within social media and behave accordingly.

6.4 Personal Internet Usage

- Employees are not allowed to access social media for personal use from WHMAT/base academy computers or devices at any time, except for the occasional professional use of LinkedIn. This includes work tablets, I-Macs, laptops etc.
- There should be no personal use of the internet during student contact time
- Visiting offensive websites using the academy's facilities is prohibited
- If staff accidentally access inappropriate material, please inform the ICT team and Head of Academy so internet filters can be updated
- **Staff must not comment about students, colleagues, the community, the trust or its academies or its partners in their personal internet use or make comments which could be viewed**

7. Education and training

7.1 Education and training in e-safety will be given high priority across WHMAT.

7.2 The education of pupils in e-safety is an essential part of WHMAT'S e-safety provision and will be included in all parts of the curriculum.

7.3 WHMAT will offer education and information to parents, carers and community users of the academies about e-safety.

7.4 Suitable training will be provided for all employees, as part of induction and subsequently during their employment in the academy. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.

7.5 Volunteers, directors and governors who use information and communication technology during their work will be offered the same training as employees.

8. Data Protection

8.1 WHMAT will ensure that its information and communication technology systems are used in compliance with current GDPR legislation and WHMAT's GDPR Data Protection Policy (see www.washwoodmat.com policies tab). It will ensure that all users are made aware of the WHMAT's Data Protection policy, including the requirement for secure storage of information.

9. Technical aspects of e-safety

9.1 WHMAT will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems and ensuring that these systems and practices are implemented.

9.2 WHMAT will undertake regular reviews of the safety and security of its information and communication technology systems.

9.3 Particular attention will be paid to secure password protection and encryption for devices located at each WHMAT site and mobile devices.

9.4 WHMAT's systems will also provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

9.5 WHMAT will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the head teacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

9.6 Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

10. Dealing with incidents

10.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's Child Protection Procedures.

10.2 Any suspicions of other illegal activity should be reported to the Head of Academy (CEO or Deputy CEO for head office staff, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved). Depending on the advice and the outcome of preliminary investigations, it may be necessary for alleged criminal activity to be reported to the police and/or may lead to the instigation of a disciplinary investigation in line with WHMAT's Disciplinary Procedure.

10.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the Head of Academy or other designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the academy's behaviour policy for pupils.

11. Policy Review

11.1 This Policy will be reviewed and amended annually by WHMAT in line with relevant guidance and good practice.

APPENDIX 1: ACCEPTABLE USER AGREEMENTS

Primary Pupil Acceptable Use Agreement	
Name of Pupil:	**Class:**

We need to be safe when we use computer and the internet. To help us stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computer/tablet
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I know that my academy looks at my use of computers/tablets.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer/tablet.

Signed (Pupil): **Date:**

Parent/carer agreement:

- I agree that my child can use the academy's IT systems and internet when appropriately supervised by a member of academy staff.
- I agree to the conditions set out above for pupils using the academy's IT systems and internet, and will make sure my child understands these.

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

Key Stage 3 – 5 Students
Acceptable use of the academy's IT systems and internet: agreement for students

Name of Student:	**Tutor Group:**

When using the academy's IT systems and accessing the internet in the academy I will not:

- Use them without a member of staff being present and/or without a member of staff's permission.
- Access only appropriate 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 member of staff.
- 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.
- I will follow the academy rules with respect to mobile phones and personal electronic devices.

When using the school's IT systems and accessing the internet in school:

- I understand that the academy will monitor my use of devices and the websites that 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 academy's IT system and internet responsibly.

Signed (student): **Date:**

Parent/carer agreement:

- I agree that my child can use the academy's IT systems and internet when appropriately supervised by a member of school staff.
- I agree to the conditions set out above for pupils using the academy's IT systems and internet, and will make sure my child understands these
- In addition I will ensure my child understands the academy rules with respect to mobile phones and personal electronic device to which I also agree.

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

Acceptable use of the academy's IT systems and internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

- I have read and agree to abide by the school's E-Safety and social media policies

- I will only use the academy's IT systems and access the internet in the academy, or outside the academy on a work device in accordance with guidelines provided by the E-Safety and social media policies.
- I understand WHMAT may monitor my use of devices and the websites that 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 the data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and IT manager know if a pupil 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 the schools IT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff /governor/volunteer/visitor):

Date: