Washwood Heath
Multi Academy Trust

E-Safety Policy

1. Introduction

1.1 The directors of Washwood Heath Multi Academy Trust have adopted this policy to help the trust 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.

1.2 This policy was adopted by the directors on 2 July 2015 and will be reviewed annually in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

2. Basic principles

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

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

2.3 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.

2.4 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.

2.5 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.

3. Roles and responsibilities

Board of Directors

3.1 The directors will consider and ratify this e-safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of particular circumstances or developments in information and communication technology. 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.

3.2 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 City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head of Academy

3.3 The Head of Academy 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.

Other employees

3.4 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 consultations 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

3.5 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

3.6 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

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

4. Acceptable use

4.1 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.
- Data Protection legislation must be followed.
- 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.

4.2 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.

4.3 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 not become online 'friends' with students and think carefully about 'friending' parents or previous students
- 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 like Facebook, Bebo, Myspace, Flickr or Twitter, 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.

4.4 Personal Internet Useage

- 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 Operation Manager and leadership team 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**

5. Education and training

5.1 Education and training in e-safety will be given high priority across the trust.

5.2 The education of pupils in e-safety is an essential part of the trust's e-safety provision and will be included in all parts of the curriculum.

5.3 The trust will offer education and information to parents, carers and community users of the academies about e-safety.

5.4 Suitable training will be provided through the academy's 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.

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

6. Data Protection

6.1 The trust will ensure that its information and communication technology systems are used in compliance with current data protection legislation and that all users are made aware of the trust's data protection policy, including the requirement for secure storage of information.

7. Technical aspects of e-safety

7.1 The trust 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.

7.2 The trust will undertake regular reviews of the safety and security of its information and communication technology systems.

7.3 Particular attention will be paid to secure password protection and encryption for devices located in the academy and mobile devices.

7.4 The trust'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.

7.5 The trust 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.

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

8. Dealing with incidents

8.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's child protection procedures.

8.2 Any suspicions of other illegal activity should be reported to the head of academy, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

8.3 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.