Bishop Walsh E- Safety Policy November 2015

Ratified by full Academy Committee	To be ratified at next meting	
Next review date		

This policy is based on the Birmingham Education model Policy 2014 whilst we await the new policy expected October 2015

This policy should be read I conjunction with the following policies:

Safeguarding Policy 2015

Anti bullying Policy

Behaviour Policy 2015

1.Introduction

1.1 The Academy Representatives of Bishop Walsh Catholic School has adopted this policy to help school meet its responsibility for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technology and digital and mobile devices.

1.2 This policy 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 technologies.

2. Basic Principles

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

2.2 The policy applies to all members of the school community, including visitors and communication users who have access to and are users of the school's information and communication technology systems or who use their personal devices in relation to their work at the school

2.3 The Academy Representatives expects the Principal to ensure that this policy is implemented, that training in e – safety is given high priority across the school, 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 the policy are submitted to the Academy Representatives for approval.

2.4 The principle context for the 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 school's behaviour and anti- bullying policies for pupils and with the rules and procedures governing the conduct of employees.

2.5 The Academy Representatives expects the Principal to arrange for this policy to be published to all employees and volunteers in the school and for the necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their age and abilities.

3. Roles and Responsibilities

Academy Representatives

3.1 The Academy Representatives will consider and ratify the 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. Academy Representatives 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 representatives

3.2 Academy Representatives are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that the City Council or other reputable specialist advice is taken on the specification for these services to ensure proper security and safeguarding of children.

Principal

3.3 The Principal is responsible for ensuring that :-

• Academy Representatives are offered appropriate support to enable this policy and its applications to be reviewed regularly and to ensure that other school policies, including that on pupils' behaviour, take account of the e – safety policy;

• the Academy Representatives are given necessary advice on securing appropriate information and communication technology systems;

• the school 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 Safeguarding Lead for safeguarding;

• there is effective consultation with all employees , and other users of the school's information and technology systems, to take account of the particular features of these systems and educational, technical and administrative needs;

• the school provides all employees with training in e –safety relevant to their roles and responsibilities and that training is also provided to volunteers and academy representatives who use information and communication technology in their capacity as volunteers or academy representatives, 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 for 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 school's information and communication technological systems;

• there is appropriate supervision of, and support for, technical staff;

• any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported the academy which commissioned the contract

Other Employees

3.4 Other employees are responsible for :-

• undertaking such responsibilities as has have been delegated by the Principal commensurate with their salary and job descriptions;

• participating in training in e –safety provided by the school 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 school 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 school's behaviour policy and the instructions given by staff.

3.6 Other users

3.6 Volunteers, including academy representatives who help in the school and who use information and communication technology systems and devices in helping the school are expected to :-

• participate in training in e- safety provided by the school and in consultations about this policy and about its application, including e – safety in 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 school for this purpose

Parents

3.7 Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school 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 use on or off the school premises.

• The schools information and communication technology systems are intended primarily for educational use and the management and administration of the school. 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 school.

4.2 Employees, volunteers and Academy Representatives should:-

• not open, copy, remove or alter any other user's files without that person's express permission and only take and / or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardian and when recording or publishing such images for educational purposes should not attach to these images any names or other personal information enabling identification.

• as far as possible communicate with pupils and parents only through the school's official communication system and not publish personal contact details through these systems.

• if they occupy a senior post in which they need to email and other messages confidential, ask the school for a separate email address for this purpose.

• if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted.

• not use personal social network sites through the school's information and communication systems.

• not open any hyperlinks in, or attachments to emails, unless the source is known and trusted.

• ensure that the data is backed – up regularly in accordance with the rules of the school's systems.

•only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems.

• not to try to install any programmes or alter any computer settings unless this is allowed under the rules of the school'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 school would expect for behaviour and conduct generally (as set out in the school's code of conduct for support staff and Teachers Standards for teachers). The school 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 school is, or will be, brought into disrepute.

5 Education and Training

5.1 Education and training in e – safety will be given high priority across the school.

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

5.3 The school will offer education and information to parents, carers and communication users of the school about e – safety.

5.4 Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. 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 and electronic materials.

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

6. Data Protection

6.1 The school 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 school's data protection policy, including the requirement for secure storage of information.

7 Technical aspects of e – safety

7.1 The school 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 these systems.

7.2 The school 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 school and mobile devices.

7.4 The school's systems will also provide for filtering for different groups of users for inappropriate content.

7.5 The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials (generally known as spam). It should safeguard children and adults against inappropriate use. It should provide the Principal 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 an incident

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 Principal, 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 the preliminary investigation, should report alleged criminal activity to the police and may also investigate disciplinary procedures.

8.3 Suspicion of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the Principal 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 disciplinary procedures for employees, or the school's behaviour policy for pupils.