BDMAT
Birmingham Diocesan
Multi-Academy Trust

Acceptable Use of Information and Communication Technology (ICT) Policy

Issued: April 2018
Next review due: Spring 2020

1.0 Context

1.1 Birmingham Diocesan Multi-Academy Trust (BDMAT) recognises that the use of internet technologies and communication devices are now seen as a vital life skill and that the use of these can help to enhance communication and the sharing of information. However, BDMAT is also aware that the use of technologies can have the potential to challenge the definitions and boundaries of learning and teaching.

1.2 Current interest technologies and electronic communications used by pupils and staff, inside and outside of BDMAT, include but is not limited to:

- Internet websites
- Virtual learning environment (VLE)
- Instant messaging (IM)
- Social networking sites (such as Facebook, Twitter)
- E-mail
- Blogs
- Video broadcasting sites
- Chat rooms
- Gaming Sites
- Music downloading sites
- Smart phones with e-mail and web applications
- Tablets and mobile phones with digital cameras

1.3 BDMAT recognises that all of these have the potential to help improve standards of learning and teaching but may equally present challenges to both pupils and staff in terms of keeping safe. The challenges include:

- Exposure to inappropriate or illegal material
- Cyberbullying via websites, social media or mobile phones
- Identity theft or invasion of privacy
- Downloading copyrighted materials
- Exposure to inappropriate advertising or financial scams (*phishing*)
- Safeguarding issues, such as grooming of under 18s or vulnerable adults
- Other illegal activities

2.0 Roles and responsibilities

2.1 Chief Executive Officer

- The Chief Executive Officer has a duty of care for ensuring the safety and e-safety of all stakeholders.
- The Chief Executive Officer and Headteachers 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 Chief Executive Officer is responsible for ensuring that relevant staff have received suitable training to enable them to carry out their e-safety roles and to train other colleagues.

- The Chief Executive Officer will ensure that there is a system in place to allow for monitoring and support of those who carry out the e-safety monitoring role.

2.2 Employees, contractors and suppliers

2.21 All teaching, non-teaching staff (central staff, volunteers, suppliers, contractors and temporary staff) are responsible for supporting safe behaviour and e-safety procedures.

2.22 All staff should be familiar with and agree to follow the Acceptable Use of ICT Policy as well as BDMAT's code of conduct and safeguarding policies.

2.23 As well as the above, all staff should do the following:

- Participate in any e-safety training and awareness raising sessions arranged by the school / BDMAT.
- Ensure they have read and signed the Acceptable Use of ICT policy.
- Act in accordance with the Acceptable Use of ICT policy.
- Report any suspected misuse or problems to their line manager; if they don't feel that they have acted appropriately with the concern they should contact the Chief Executive Officer or Finance Director and / or use the Whistle Blowing policy
- Refrain from making negative comments about BDMAT, its schools and stakeholders via any electronic communications (e.g. social networking sites, messaging apps).
- Ensure that any electronic communications with other stakeholders are on a professional level and adhere to the Acceptable Use of ICT policy.
- Help to educate pupils in keeping themselves safe.
- Help pupils to understand and follow the Acceptable Use of ICT policy and procedures.
- Monitor pupils' use of electronic devices, such as mobile phone and tablets, in lessons and other relevant activities, and implement current policies with regards to these devices.

2.3 Pupils

- All pupils should be taught to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- All pupils should be taught to understand the importance of adopting good e-safety practice when using electronic communication outside of BDMAT.

3.0 Key terminology

3.1 Acceptable Use Policy (AUP)

An acceptable use policy (AUP) is a document that outlines a set of rules to be followed by all users of a set of computing resources, which could be a computer network, website or computer system. An AUP clearly states what the user is and is not allowed to do with these resources.

3.2 Child Protection and Safeguarding

This is part of safeguarding and promoting welfare. This refers to the activity that is undertaken to protect specific children who are suffering, or likely to suffer significant harm.

Safeguarding and promoting the welfare of children is:

- Protecting children from harm
- Protecting children from that which is not in their best interest
- Preventing the impairment of children's health and safety

3.3 Children and under 18s

The Children Act 1989 states the legal definition of a 'child' as a 'person under the age of 18'.

3.4 Cyberbullying

3.41 This refers to bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers and tablets, as well as communication tools including social media sites, text messages, chat and websites.

3.42 Examples of cyberbullying include mean text messages or emails, rumour sent by texts, email or social networking sites, embarrassing pictures (sexting) or videos posted on websites, and the creation of fake profiles.

3.5 Duty of care

This is the legal obligation to safeguard others from harm while they are in your care, using your services or associated with your activities.

3.6 Digital media

Digital media is digitised content that can be transmitted over the internet or computer networks. This can include text, audio, video and graphics.

3.7 E-Safety

The safe and responsible use of internet technology and other electronic communications.

3.8 E-safety Coordinator

The e-safety coordinator is responsible for coordinating the whole school e-Safety approaches, supporting and raising awareness with the wider community, promoting a safe and responsible e-Safety culture and acting as the lead for dealing with e-Safety issues that arise.

3.9 Information and Communications Technology (ICT)

ICT (information and communications technology – or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on.

3.10 Stakeholders

All pupils, staff, volunteers, visitors and contractors who attend, visit or provide services for BDMAT either centrally or in its schools.

3.11 Social media

Websites and applications that enable users to create and share content or to participate in social networking.

3.12 Social networking

The use of websites and other internet services to communicate with other people and make friends.

4.0 Policy Statement

4.1 This Acceptable Use of ICT Policy relates to all stakeholders of BDMAT (including pupils, staff, volunteers, visitors and contractors) who have access to, and are users of internet technologies and electronic communications both in and out of BDMAT and its schools where actions relate to BDMAT activities or the use of BDMAT ICT systems.

4.2 BDMAT seeks to maximise the educational benefit that can be obtained by internet technologies and electronic communication devices, while at the same time minimising any associated risks.

4.3 Safety and well-being is the collective and individual responsibility of all its stakeholders.

4.4 BDMAT aims to ensure that regardless of age, gender, race, ethnicity, religion or beliefs, sexual orientation, socio-economic background, all stakeholders have a positive and safe learning, teaching and working experience.

4.5 As part of this policy, BDMAT will:

- Promote and prioritise e-safety for all members.
- Establish an understanding of roles and responsibilities in respect of e-safety and ensure everyone is provided with appropriate learning opportunities to recognise, identify and respond to any concerns regarding to the use of internet technologies and other electronic communications.
- Ensure that appropriate action is taken in the event of any e-safety concerns and support the individual(s) who raise or disclose the concern.
- Ensure that confidential, detailed and accurate records of all e-safety concerns are maintained and securely stored.
- Ensure that robust e-safety arrangements and AUPs are in operation.

4.6 This policy is applicable to all stakeholders of BDMAT.

4.7 Failure to comply with this policy and procedures will be addressed immediately and may ultimately result in dismissal for staff or exclusion for pupils from BDMAT.

5.0 Policy Review

This policy will be reviewed every two years in the summer term or following any updates in relevant policies or procedures. Feedback is collected annually from all stakeholders. This policy will be reviewed by the Finance Director and Chief Executive Officer.

6.0 Code of conduct

6.1 This policy:

- Assists stakeholders in working safely and responsibly and monitoring their own standard and practice;
- Sets clear expectations of behaviour and codes of practice relevant to e-safety and use of ICT;
- Supports stakeholders by giving a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

7.0 Managing internet access and information systems

7.1 To ensure that BDMAT's information systems remain safe:

- The security of BDMAT's information systems will be reviewed regularly, and at least annually.
- Virus protection will be updated when updates are issued.
- Firewalls and filters will be used at all times.
- Unapproved software will not be allowed in work areas or attached to emails.

7.2 BDMAT's equipment and systems must not be used:

- For any form of harassment of individuals, including colleagues, clients and other stakeholders.
- To download, access, record and/or store material that could be considered racist, sexist, homophobic or likely to be in contravention of discrimination, bullying or harassment legislation.
- To access adult or pornographic material.
- To upload any inappropriate content (including copyrighted or indecent material).
- To install any programs without the prior permission of a designated member of staff.
- To attempt to circumvent or 'hack' any systems.

7.3 BDMAT reserves right to view all material (including email of a personal nature) stored in its computer systems.

8.0 Email

- Pupils and staff must immediately tell a designated member of staff if they receive an offensive / inappropriate email.
- Staff will only use official work-provided email accounts to communicate with other stakeholders (including pupils, parents/carers and third parties).
- Emails must not be used to forward inappropriate messages or content to any individual.

9.0 Emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in BDMAT is allowed.

10.0 Filtering

- BDMAT and its schools' broadband access will include appropriate filtering.
- If a pupil or a member of staff discovers an unsuitable site, the URL will be reported to the Headteacher who will record the incident and escalate the concern as appropriate.
- The e-safety coordinator will ensure that regular checks are made to ensure that the filtering methods selected are effective.

11.0 Mobile phones and personal devices (including laptops and tablets)

The use of mobile phones and other personal devices by pupils and staff in school will be decided by the individual school. However, BDMAT advises that:

- Mobile phones and personal devices will not be used by staff or pupils during lessons unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Electronic devices of all kinds that are brought into school are the responsibility of the user. BDMAT does not accept responsibility for the loss, theft or damage of such items.
- Staff and other stakeholders must not use their personal phones or devices to contact any pupil under 18 years of age. (unless in extreme circumstances such as COVID19 for welfare calls under the direction of the Headteacher)
- Staff and other stakeholders must never use their personal phones or devices be used to take images of pupils.
- Staff and other stakeholders must not use their personal phones or devices to contact parents or pupils (unless in extreme circumstances such as COVID19 for welfare calls under the direction of the Headteacher)

12.0 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and due regard will be made of the General Data Protection Regulations when they come into force.

13.0 Published content and BDMAT websites

- The contact details on the BDMAT and individual school websites should be the school address, email and telephone number. Other stakeholder personal information will not be published.
- The Chief Executive Officer will take overall editorial responsibility and ensure that content is accurate and appropriate. The Chief Executive Officer will delegate to the individual school's Headteacher editorial responsibility for the school website.

14.0 Publishing images of pupils

- Photographs of pupils will be selected carefully and will not enable an individual pupil to be identified unless the parent / carer has given permission
- The full names of pupils will not be used anywhere on the website or social media networks.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the website or on social media networks.
- Written consent will be kept by BDMAT/schools where the images of pupils are used for publicity purposes. The permission must clearly state what the parent / carer gives permission for e.g. for the school's website only; for BDMAT's website; for publicity information etc.

15.0 Social media and social networking

- All pupils will be advised never to give out personal details of any kind which may identify them and/or location. Examples would include real name, address, mobile number, school attended, instant messaging and email address.
- All pupils and staff will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- All pupils and staff will be advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff are required to not post entries that are publicly accessible, which contain negative references to BDMAT or its schools, its staff, business activities, pupils, parents / carers or services.
- Staff must not conduct themselves at any time in a way that is detrimental to BDMAT.
- Staff must take care not to allow their interaction on social networking websites to damage working relationships between members of staff and the BDMAT's clients and third parties.

- Staff must not 'add' any pupil aged under 18 years of age to their personal social networks with the exception of family members
- Concern regarding pupil's use of social networking, social media, and personal publishing sites (in or out of school) will be raised with their parent/carers, particularly when concerning pupil underage use of sites.

APPENDIX

Acceptable Use of ICT Policy

- I have read and understood the Acceptable Use of ICT Policy.
- I agree to abide by the Acceptable Use of ICT Policy.
- I understand that I have a responsibility for my own and others' e-safety, especially regarding under 18s.
- I understand that it is my responsibility to ensure that I remain up to date and read and understand BDMAT's most recent Acceptable Use of ICT Policy.
- I understand that I must ensure that I comply with BDMAT's Privacy Policy.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Signed: _____

Date: _____