Education Central Multi Academy Trust

SOCIAL MEDIA, SOCIAL NETWORKING AND E-SAFETY POLICY and PROCEDURE

Author	**ECMAT Human Resources**
Approved	**12th May 2014**
Date	**May 2014**
Version	**1**
Review	**September 2016 (unless legislative or national changes dictate that an earlier review is required)**

Contents

1. Introduction

1.1. This Policy applies to all those who benefit from an Internet service at Education Central Multi Academy Trust (ECMAT). It applies to all permanent, fixed term and temporary Academy based employees; to temporary and agency staff; to contractors; to all third parties working for the ECMAT Family; to volunteers and any other parties using ECMAT and Academies Internet services. This Policy applies to these parties whatever their purpose, whether or not the Internet connection is for their work or for private use. All use of the Internet must be in accordance with this Policy and related policies.

1.2. The over-riding objective is that pupil well-being is never adversely affected through the use of Communications and Information Technology equipment.

1.3. Unless the context otherwise demands, "ECMAT" means the central ECMAT organisation and each of its constituent Academies.

1.4. The appendices to this Policy include best practice, protocols and general guidance information for staff. They also include codes of practice, agreement forms and protocols in respect of pupils' social networking, social media and Internet use.

1.5. This Policy applies whenever ECMAT provides an Internet service, with the exception of public access Internet provision. It applies whenever the Internet is accessed through an ECMAT connection, whether the computer equipment or smartphone is owned by ECMAT or not.

1.6. ECMAT employees are required to treat members of the public and other employees in accordance with ECMAT's Equal Opportunities statement. ECMAT encourages good relationships in the workplace and a safe environment in which all individuals are respected and able to work effectively together. To achieve this, individuals need to work within certain rules and standards of behaviour.

1.7. This Policy aims to protect the good reputation of ECMAT and the ECMAT Family of Academies to promote best use of Internet facilities for achieving Academy objectives.

1.8. ECMAT may after appropriate consultation with recognised trades unions amend this Policy and Procedure at any time if it considers it appropriate to do so.

1.9. The Headteacher will ensure that all employees are aware of this Policy and have read, understood and agreed to comply with the Policy. The information in this Policy is designed to provide employees with a guide to acceptable use, which they are required to follow. Failure to do so may result in disciplinary action under The Academy's disciplinary procedure. The Headteacher of an Academy must ensure that employees have ready access to this procedure, either electronically or in the form of a paper copy in that Academy's office. Copies should also be displayed on notice boards in Academy staff rooms or other areas in the Academy where employees meet together e.g. Academy Internet site.

1.10. The Policy and any amendments have been adopted following consultation with representatives from both Teaching and Support Staff trade unions, and ratified by the ECMAT Board and may be amended from time following further consultation.

1.11. Any amendments will be promptly notified to staff via the ECMAT Board.

2. Communications and IT Equipment

2.1. ECMAT provides information and communications technology systems to enable its employees to work efficiently.

2.2. In addition, ECMAT provides access to the vast information resources of the Internet and the Web to help us all do our job and be well informed. The facilities that the Academy provides represent a considerable commitment of resources. This Policy is designed to help employees understand expectations for the use of those resources and to ensure that all staff use those resources wisely, appropriately and legally.

2.3. 'Communications and IT equipment' refers to, but is not limited to, cameras, computers, tablets, Internet access, remote access connections, email servers, file storage, webmail, personal digital assistants (Blackberrys, IPADs IPAQs, Smart-Phones, Palm Pilots, etc.), telephones, mobile phones and computing and networking facilities owned and operated by ECMAT/the Academy.

2.4. Communications and IT equipment enable staff to communicate both internally and externally and to store information, including personal or sensitive information. All staff and other users are therefore expected to use the systems provided in ways which:

- Comply with legislative requirements (e.g. data protection, equality legislation, health and safety, etc.)
- Enhance efficiency and productivity
- Enhance the reputation of ECMAT and its Family of Academies.

3. Data Protection

3.1. ECMAT is registered under the Data Protection Act 1998. Employees, trustees and directors and governors are required to ensure that information and data held on the Academy's computer systems complies fully with the principles of this Act. The Act requires that anyone who inputs, stores or uses personal information must ensure that the information (e.g. names, addresses, other information kept on individuals) is:

- accurate and up to date
- only kept for legitimate reasons
- only kept for as long as is necessary
- only used for legitimate purposes
- not passed on to third parties without the consent of the individual
- secure

4. Social Media & Social Networking

4.1. *"Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny."* – Guidance for Safer Working Practice for Adults who Work with children and Young People – DCSF, 2009.

4.2. This Policy covers all forms of social media, including Facebook, Twitter, LinkedIn, Wikipedia, other social networking sites and other Internet postings. It applies to the use of social media for both business and personal purposes, during working hours and in personal time to the extent that it may affect the business operations of ECMAT. The Policy applies both when the social media is accessed using ECMAT information systems and also when access using equipment and/or software belonging to employees or others.

4.3. Social networking applications include but are not limited to the following (the principles of this Policy also apply to other types of online presence such as virtual worlds):

- Blogs, for example 'Blogger'
- On-line discussion forums, such as 'Ning'
- Collaborative spaces, such as 'Wetpaint'
- Media sharing service, such as 'YouTube'
- Micro-blogging applications, such as 'Twitter'

4.4. Staff must not use social media in a way that might breach any ECMAT Policy, any express or implied contractual obligations, legislation, or regulatory requirements. In particular, use of social media must comply with:

- the Electronic Communications and Information Systems Standards
- ECMAT's Equal Opportunities and Anti-Harassment Policies
- rules of relevant regulatory bodies
- contractual confidentiality requirements
- other key policies/requirements

Whilst the appropriate use of social media can be positive and productive, it is important to be aware that it can pose significant risks to the Academy, staff and pupils. The use of social networking applications has implications for our duty to safeguard children; young people, vulnerable adults and employees, and other risks include disclosure of confidential information and intellectual property, damage to the Academy's reputation and the risk of legal claims. To minimise these risks this Policy sets out the rules applying to the use of social media.

4.5. The purpose of this Policy is to ensure:

- All staff and pupils are safeguarded against allegations which may arise through inappropriate use of social media and networking sites.
- The reputation of ECMAT and staff is not adversely affected.
- ECMAT is not exposed to legal and governance risks.

4.6. ECMAT considers the use of social media and social networking sites to be a strictly personal activity.

4.7. ECMAT staff are not permitted to access any social media for personal use during working time or use the ECMAT information systems at any other time for personal use. Academy information systems and media equipment must only be used for ECMAT business. Staff must not use online social networking sites such as Facebook /Twitter/MySpace, etc., during working time.

4.8. Staff must never engage in social networking with a student (except with a student who is a member of that employee's immediate family). All electronic communications with pupils should be done via ECMAT email which will be regulated. To engage in social networking with pupils leaves staff vulnerable to accusation and speculation. Staff must take all steps necessary to safeguard themselves. Staff who suspect that a pupil seeks an inappropriate relationship with them must bring this to the attention of their line manager immediately. Failure to do so, could lead to disciplinary action.

4.9. Staff must not give pupils their private mobile phone number (except to a pupil who is a member of that employee's immediate family).

4.10. Staff must not phone or text pupils or have pupils phone or text details.

4.11. Staff must not give pupils their private email addresses or ask pupils for their private email address (except a pupil who is a member of that employee's immediate family).

4.12. If a member of staff suspects that a pupil has obtained that employee's private e-mail address or mobile 'phone number, that employee must bring this to the attention of their line manager as soon as possible.

4.13. References to places of work, ECMAT, Academy, telephone numbers or addresses, should not be given on websites.

4.14. Staff should not take, use or post photographs of pupils or staff in their work environment unless this is for professional ECMAT business.

4.15. No reference to roles at work, job titles or confidential information should be given

4.16. Colleagues should not be subjected to inappropriate or unwanted reference either in writing or photographs. Staff must not communicate with pupils through private emails. Staff can use ECMAT email systems to communicate with pupils in relation to Academy business only. In certain circumstances e.g. Academy trips, staff will be given an ECMAT mobile phone and will receive guidance on how this can be used.

4.17. Staff are strongly advised not to enter into social networking with former students. Circumstances may lead staff to be vulnerable to accusation and speculation which may lead to disciplinary action and/or dismissal.

4.18. Staff should never name students or make reference to a student's personal circumstances. Safeguarding/Child Protection breaches can easily be made by the use of an innocent or thoughtless comment.

4.19. If required or permitted to use social media sites in the course of performing their duties for or on behalf of ECMAT, staff should ensure that such use has appropriate prior authorisation and that it complies with the standards set out in this Policy.

4.20. Staff must be aware that by identifying themselves as a member of ECMAT they become, to some extent, a representative of the Academy and everything they post has the potential to reflect on ECMAT and its image. Therefore, should staff identify themselves as Academy members they take on the responsibility for representing ECMAT in a professional and positive manner. Defamatory statements about ECMAT or colleagues can lead to disciplinary action or even legal action.

4.21. In using social media staff must not:

- Make disparaging or defamatory statements about ECMAT its employees, pupils, clients, customers, or suppliers
- Harass, bully or unlawfully discriminate in any way
- Use data obtained in the course of their employment with ECMAT in any way which breaches the provisions of the Data Protection Act 1998
- Breach copyright belonging to ECMAT
- Disclose any intellectual property, confidential or commercially sensitive information relating to ECMAT or its business
- Make statements or use social media communications which cause, or may cause, harm to ECMAT's reputation or otherwise be prejudicial to the interests of ECMAT

4.22. Staff should make it clear in personal postings that they are speaking on their own behalf, in particular write in the first person and use a personal e-mail address. If a staff member discloses that he/she is an employee of ECMAT, they must state that their views do not represent those of their employer. For example, staff could state, "the views in this posting do not represent the views of my employer".

4.23. Staff are personally responsible for what they communicate in social media. Often materials published will be widely accessible by the public and will remain accessible for a long time. If staff are uncertain or concerned about the appropriateness of any statement or posting, they should discuss it with their line manager before making the post.

4.24. Staff should be aware that social networking sites have varying levels of security and as public sites all are vulnerable to breaches in security and to surveillance by security services in UK and abroad.

5. Internet use

5.1. Security

This Policy is intended to minimise security risks. These risks might affect ECMAT information resources and IT equipment, an authorised Internet user and the public. In particular these risks arise from:

- Hacking and other unauthorised access to ECMAT systems or other computer systems
- The wrongful disclosure of private, sensitive, privileged, confidential and commercially sensitive information
- The exposure of ECMAT systems to malicious or harmful software
- The use of ECMAT systems or other computer systems to access inappropriate or offensive material (and other risks such as bullying or fraud associated with such inappropriate material)
- Vicarious liability of ECMAT for commitments made by individuals on the Internet

5.2. Monitoring

All use of the Internet, both business and private, may be recorded and reported on. ECMAT reserves the right to monitor, at any time, all Internet usage, including Internet browser history files, storage of temporary Internet files and any downloads from an Internet site and emails, including deleted emails, and the systems upon which such emails are stored and circulated.

5.2.1. ECMAT reserves the right to monitor, at any time, internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following reasons:

- To investigate or detect the unauthorised use of the systems, e.g. to check that this Policy is being observed, that no discriminatory or offensive content appears in emails, etc.
- To maintain an adequate level of security for ECMAT computer systems.
- To detect any computer viruses.
- To check mailboxes of absent employees.

5.2.2. It is the practice within ECMAT for all staff to allow their manager (and others as agreed with management) access to Outlook calendars and email inboxes. In relation to accessing calendars, this is to help planning and to help ensure staff safety whilst working away from an ECMAT site and working alone. Access to email inboxes is required in the event that staff receive important emails during periods of absence.

5.2.3. While an email that is clearly private does not fall within the definition of a communication that is relevant to ECMAT's business, ECMAT maintains a right to monitor such a communication where there is a reasonable suspicion that the content breaches ECMAT's Policy and or the member of staff's position of trust.

5.2.4. To exercise its right under the regulations, an organisation must have made all reasonable efforts to inform every person who may use the system that interception may take place. We believe that the communication of this Policy to all employees meets this requirement.

5.3. Access and Misuse

ECMAT's Internet facilities are provided for ECMAT business purposes and access must be authorised by an appropriate manager. Access is granted only on condition that the individual formally agrees to the terms of this Policy and the related codes of practice.

To support various ECMAT policies and duties, access to certain web sites is restricted, particularly those which display criminal, hate, sexually explicit, racist and other inappropriate material. In order to implement this Policy and to further its objectives, ECMAT reserves the right to block access to certain Internet sites/categories without warning. The Academy may also take temporary measures to block or change the access to a particular Internet site/category.

5.3.1. Certain activities and Internet sites are prohibited to safeguard the Internet service and to further the objectives of this Policy. Misuse of ECMAT's computing facilities may result in disciplinary or criminal proceedings. Misuse constitutes (but is not limited to) the following:

a) Using Internet facilities to break the law or incite crime.

b) Gaining unauthorised access, or making unauthorised modifications, to computer material (hacking).

c) Entering into contractual obligations on behalf of ECMAT over the Internet, unless the transactions are formally authorised in writing by line managers having acted in accordance with the approved corporate procedure.

d) Accessing, using, extracting, storing, distributing, printing, revealing or otherwise processing information which contravenes the law or ECMAT policies, particularly policies on harassment and discrimination.

e) Distributing copyright material in breach of copyright.

f) Distributing defamatory material.

g) Unlawfully disclosing any sensitive business information, commercially sensitive information or personal information.

h) Transferring information with a classification higher than NOT PROTECTIVELY MARKED over the Internet. (This is a general standard measure in respect of online information which means authorisation for its use is not required.)

i) Attempting to access sites which are blocked or trying to circumvent any of the controls which block access to Internet sites.

j) Using another individual's user identity or password.

k) Attempting to discover another person's username and password, by any means.

l) Attempting to monitor or tamper with another user's electronic communication or data, or reading, copying, modifying or deleting another user's data without the explicit agreement of that user, or their Manager. (Except in the case of electronic mail messages where messages sent and received can be copied and/or monitored).

m) Attempting to circumvent by any means the computer or network security.

n) Using the computer systems (such as electronic mail) to act abusively towards others (including individuals, groups, companies or any other organisation) whether internally or externally.

o) Knowingly running and installing on any computer or network, or giving to another user, a program or macro intended to disrupt or damage in any way the computer systems and/or network operations, its files, programmes, data, or any related peripheral or device.

p) Violating terms and conditions of software copyrights and agreements, including making unlawful copies of software.

q) Installing any software by whatever medium (e.g. data sticks, CD-ROM or data transfer) not purchased on behalf of or provided, virus checked and approved by ECMAT/the Academy. This includes any software from previous employers or from home computers. The installation of software where the origin of the software is not known is strictly prohibited.

r) Using the computer systems for any activity not related to work for ECMAT (exemptions to this include: collecting personal emails, e-banking or searching other appropriate websites during a recognised break with the prior permission of your manager), or for personal financial gain.

s) Relocating or re-allocating computer equipment without permission.

t) Deliberately wasting computer resources such as game playing or sending “junk” or “chain” mails (either electronic or printed) during working hours.

u) If a member of staff is allocated a laptop, tablet or portable computer, that employee is responsible for ensuring the safe keeping of this equipment whilst out off site. Under no circumstances should this equipment be left unattended in a public place, or in public view. Further, the employee must ensure that all security systems and precautions have been activated to safeguard the portable computer.

5.3.2. Producing, downloading or distributing sexually explicit or offensive material in any form, electronic or otherwise (e-mail, blogging, picture, file, printed-output, etc.), which may be considered abusive or derogatory to individuals on the basis of race, ethnicity, religion, gender, sexual orientation, gender re-assignment, disability, age, etc., is a violation of ECMAT’s Equal Opportunity Policy. Any such action will be considered as gross misconduct.

5.3.3. If staff members find themselves connected accidentally to a site that contains sexually explicit, offensive or illegal material, they must immediately disconnect from that site and notify their manager as soon as possible.

5.3.4. Staff should not subscribe to chat rooms, dating agencies, messaging services, blogs or other online subscription Internet sites unless they pertain to work duties.

5.3.5. Staff may be held responsible for damage to equipment, programs or data, and may be held accountable for any licensing infringements if they do not comply with this Policy.

5.4. Private use

Some private use, which is not related to ECMAT work, is allowed within certain limits as described [e.g. see clause 5.3.1(r)]. This is to be viewed as a privilege and, if evidence of abuse is found, appropriate disciplinary action will be taken against individuals concerned.

5.5. Passwords

All systems require an authenticated User ID/password combination prior to gaining access. Staff should not use another person's login ID (username/password). If staff require access to another employee's computer system, a request must be submitted to their line manager who will arrange for temporary access. In order to protect information, staff must set appropriate passwords on sensitive or confidential data and keep passwords safe. Staff are responsible for the security of their password(s) and should not divulge them to anyone. Giving another person a username and password is not permitted, as staff are held accountable for all actions under their username. Should a staff member believe that another person knows their password, it should be changed immediately.

5.6. Computer Usage

Computers should be fully shut down and turned off at the end of each day. This includes turning off the screens. To prevent unauthorised access to files, staff should ensure that they log out, or otherwise secure their computer if they are away from their desk.

5.7. Data security

5.7.1. To prevent accidental loss of data, staff should ensure that all files are saved to shared folders so they are regularly backed up. Please note that documents saved on a PC or laptop hard drive will NOT be backed-up. Information stored on data stick must not contain personal or sensitive data and must be effectively encrypted. Network security must be maintained. No attempt must be made to disable, defeat or circumvent ECMAT firewalls or similar network security facilities.

5.7.2. Note that firewall software can automatically disconnect Internet connections when this is necessary to protect the service. No Internet user may use the Internet deliberately to propagate any virus, worm, Trojan Horse, spyware, malicious code or unauthorised mobile code.

5.7.3. Only the Academy's Internet manager/IT Manager can:

a) Connect any part of ECMAT's network to the outside world.

b) Authorise use of technological applications and peripherals, including telephones and cameras, which connect to the Internet through ECMAT Internet connections.

c) Manage any connection which links ECMAT's network to the outside world. Internet users are not allowed independently to connect PCs or servers which are already connected to the ECMAT network or to the Internet or to any their external system.

5.7.4. In exceptional circumstances, connections may be allowed through independent dial-up devices (modems) or other methods. These exceptions must always be authorised in advance by the relevant Headteacher/IT Manager.

5.7.5. Internet connections using ECMAT's telephone network are not allowed.

5.8. Discipline

Any employee who contravenes the rules in this Policy will be disciplined under the Academy's disciplinary procedure. Any employee who uses IT resources for illegal activity or to access pornographic, offensive or other improper material, or make inappropriate use of the Internet, will be disciplined and the activity will be reported to law enforcement agencies. Any employee who uses IT resources for the distribution of defamatory material will be disciplined. It is possible that the disciplinary procedure could result in dismissal. When there is evidence of a criminal offence, the police will be informed.

6. E-Safety - Introduction

6.1. ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Education Central Multi Academy Trust (ECMAT) needs to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

6.2. Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

6.3. Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

6.4. At **(Insert name of Academy)** we understand the responsibility to educate our pupils one e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

6.5. **(Insert name of Academy)** holds personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be

used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the Academy. This can make it more difficult for this Academy to use technology to benefit learners.

Everybody in ECMAT and in each Academy has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement see appendix 1 and section 9 (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the Academy (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

7. Monitoring

7.1. Authorised ICT staff may inspect any ICT equipment owned or leased by ECMAT at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

7.2. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving ECMAT employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain ECMAT business related information; to confirm or investigate compliance with ECMAT policies, standards and procedures; to ensure the effective operation of ECMAT ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998; or to prevent or detect crime.

7.3. ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent, in order to deal with any business-related issues retained on that account.

7.4. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

7.5. Please note that personal communications using Academy ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

8. Breaches

8.1. A breach or suspected breach of policy by an ECMAT employee, contractor or pupil may result in the temporary or permanent withdrawal of ECMAT ICT hardware and/or software and/or services from the offending individual.

8.2. Any policy breach is grounds for disciplinary action in accordance with the Academy Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings which may lead to a referral through the independent safeguarding authority.

8.3. The Information Commissioner's Office powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

8.4. The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

8.5. Incident Reporting

Any security breaches or attempts, and any loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported ECMAT's ICT or e-Safety Co-ordinators as appropriate.

9. Acceptable Use Agreements

There is a requirement that all users of digital equipment and information technology understand their responsibilities within this policy. As such acceptable use agreements will need to be read and signed. For Staff, Governors and Visitors (see **Appendix 1**).

Copies of signed agreements should be returned to the Academy Business Manager **(insert name)** for filing and record purposes.

10. Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) must be checked in advance for any viruses using Academy provided anti-virus software before using them
- No employee shall interfere with any anti-virus software installed on ECMAT ICT equipment
- If a machine is not routinely connected to the Academy network, its users must make provision for regular virus updates
- Any employee who suspects that there may be a virus on any ECMAT ICT equipment, must forthwith stop using the equipment and contact the relevant Headteacher or IT Manager as soon as possible.

11. Data Security

The accessing and appropriate use of ECMAT data is something that ECMAT takes very seriously.

11.1. Security

- ECMAT gives relevant staff access to its Information Systems, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing ECMAT data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use for which they sign and which are then kept on file
- The term “Visitors” covers staff and Local Advisory Board members who must sign the same document. This is held by the Senior Information Risk Owner (SIRO)
- The Leadership Team has identified Senior Information Risk Owner (SIRO) and Information Asset Owner (IAO)
- Staff must keep all ECMAT related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it must be kept locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used
- Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

11.2. Restrictions on access

- Appropriate labelling of data should help Academies and ECMAT secure data and so reduce the risk of security incidents
- Labeling must be applied in accordance with guidance from the relevant Academy's Senior Information Risk Owner (SIRO)
- Most learner or staff personal data will be classed as "Protect" but some will be classed as "Restricted"

11.3. Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and ECMAT's response. The SIRO is a member of the senior leadership team and has the following responsibilities:

- to own the information risk policy and risk assessment
- to appoint the Information Asset Owner (IAO)
- to act as an advocate for information risk management

The Office of Public Sector Information has produced ***Managing Information Risk***, [**http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf**] to support their role.

The SIRO in this Academy is **(Insert name of SIRO within the Academy)**

11.4. Information Asset Owner (IAO)

Information that is sensitive needs to be protected. This includes the personal data of learners and staff; such as assessment records, medical information and special educational needs data. (**Insert name of Information Asset *Owner*** *e.g. this may be the Business Manager or person responsible for holding sensitive information within the relevant Academy*) has been identified as the Information Asset Owner.

The role of our IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected and to apply the appropriate protective marking following discussion with the SIRO (e.g. any data that can be linked to an individual, pupil or staff etc.)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained
- how information is disposed of

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although this role has been explicitly identified, the handling of secured data is everyone's responsibility – whether they be an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct and/or legal action.

12. Disposal of Redundant ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed.
- Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998

http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- Each Academy and ECMAT will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- Each disposal record will include:
    - Date item disposed of
    - How it was disposed of e.g. waste/recycling
    - Authorisation for disposal, including:
        - verification of software licensing where appropriate
        - record of internal disposal or written guarantee from disposal company
- Any redundant ICT equipment being considered for recycling will have been subject to a recent electrical safety check and hold a valid PAT certificate

13. Email

The use of email within ECMAT is an essential means of communication for both staff and pupils. In the context of ECMAT, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between ECMAT and the Academy Family on different projects, be they staff based or pupil based, within the Academy or international. ECMAT recognises that pupils need to understand how to style an email in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experience of sending and receiving emails.

13.1. Managing e-Mail for staff and pupils given access to Academy email or Virtual Learning Environment (VLE)

- Each Academy and ECMAT gives all staff their own e-mail account to use for all ECMAT business as a work based tool. This is to minimize the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The ECMAT email account should be the account that is used for all Academy and ECMAT business
- Under no circumstances should any member of staff use his/her personal email address to contact pupils, parents or conduct any Academy or ECMAT business
- All emails should be written and checked carefully before sending, in the same way as a letter written on Academy or ECMAT headed paper
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account only when appropriate
- Pupils may only use ECMAT approved accounts on any ECMAT system and only under direct teacher supervision for educational purposes
- Emails created or received during the course of employment by ECMAT will probably be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Therefore employees must actively manage their ECMAT email account(s) as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupils have their own individual Academy issued accounts on the **(insert name; e.g. Academy's VLE)**
- The forwarding of chain letters is not permitted on the Academy VLE
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail. This information should then be passed to the appropriate manager for further investigation

- Staff must inform (the E-Safety co-coordinator) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT Scheme of Work
- Regardless of the means by which ECMAT e-mails are accessed (whether directly, through webmail when away from the office or on non-Academy hardware) all the Academy e-mail policies apply

13.2. Sending Emails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to Section 13.4 of this Policy entitled "Emailing Personal, Service, Confidential or Classified Information"
- The sender of an email should use her/his own e-mail account in order to be identified as the originator of a message
- If required to send an email from someone else's account, the sender must always identify him/herself as the sender
- The number and relevance of email recipients, particularly those being copied in, must be kept to the minimum necessary and appropriate
- Attachments must not be unnecessarily sent or forwarded. Whenever possible, the location path to the shared drive should be sent instead of sending attachments
- Any incoming or outgoing email greater than twenty megabytes (including any attachments) is likely to be stopped automatically.
- ECMAT email is not to be used for personal advertising

13.3. Receiving e-Mails

- Emails should be checked on a regular basis
- Use caution when opening attachments and be sure not to open attachments from untrusted sources
- The email system should not be used to store attachments - business related work should be detached from emails and saved to the appropriate shared drive/folder

13.4. E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail. E-mailing confidential data is not recommended and should be avoided where an alternative exists. The use of secure data transfer systems should always be investigated first. Full training on using these systems will be provided by ECMAT and as part of directed time
- Internet based webmail services – such as Hotmail and BT Internet – are unsuitable for sending e-mail containing sensitive information
- Where no alternative to email is available express managerial consent to transmit such data via email should be obtained (ECMAT will ensure this process doesn't increase workload)

- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
- When sending an e-mail containing personal or sensitive data a security classification should be entered in the first line of the e-mail. For e-mails to do with information about a pupil, for example, '**PROTECT – PERSONAL'** should be entered on the first line of the e-mail. This also needs to go on the top of any documents that are sent (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc.).

14. Equal Opportunities

ECMAT endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of our E-Safety rules.

ECMAT recognizes that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues. ECMAT will provide all necessary resources to meet this requirement.

When raising E-safety awareness ECMAT, in consultation with staff, will consider carefully the needs of pupils with poor social understanding - particularly during group interactions. Such work for these pupils will be appropriately planned and managed.

15. E-Safety

15.1. E-Safety - Roles and Responsibilities
(delete elements that are not being taught in the Academy).

As E-Safety is an important aspect of strategic leadership within ECMAT. In each Academythe Headteacher and LAB have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinator/s, and their workplace base can be found in the annex (**create annex for this purpose**) who have been designated this role as a member of the senior leadership team. ECMAT will distribute this info and ensure it remains updated.. It is the role of the E-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as ECMAT, CEOP (Child Exploitation and Online Protection).

Senior Management and LAB members will be kept updated by the Head/ E-Safety co-ordinator and all LAB members have an understanding of the issues and strategies at each Academy in relation to local and national guidelines and advice.

This policy, supported by the ECMAT's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole ECMAT community. It is linked to the following mandatory ECMAT policies: child protection, health and safety, home–Academy agreements, and behaviour/pupil discipline (including the anti-bullying) policy.

Use of the email, ICT and related systems by the recognised trade unions is permitted under the facilities agreement. Staff e-mails that are marked 'personal' and/or 'union business' will not be read by ECMAT management without prior consent.

15.2. E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- ECMAT has a framework for teaching internet skills in ICT/ PSHE lessons
- ECMAT provides opportunities within a range of curriculum areas to teach about E-Safety
- Educating pupils on the dangers of technologies that maybe encountered outside ECMAT is done informally when opportunities arise and as part of the E-Safety curriculum
- Pupils will be made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modeling and activities
- Pupils will be made aware of the impact of Cyber bullying and advised how to seek help if they are affected by any form of online bullying. Pupils are also be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

15.3. E-Safety Skills Development for Staff

Our staff will receive regular information and training on E-Safety issues. Union Learning Reps and management, will together identify ICT training and other development opportunities for all staff to ensure that knowledge in this area is kept up to date

- New staff will receive information on ECMAT's acceptable use policy as part of their induction

- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and receive training on what to do in the event of misuse of technology by any member of the ECMAT community (see enclosed flowchart)

- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas

15.4. Managing ECMAT E-Safety Messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used

- The E-Safety policy will be introduced to the pupils at the start of each Academy year and through ongoing curriculum activities

- E-Safety posters will be prominently displayed within each Academy.

16. Incident Reporting, e-Safety Incident Log & Infringements

16.1. Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported the ECMAT's relevant SIRO, IAO or e-Safety co-ordinator as appropriate.

16.2. E-Safety Incident Log

All e-safety incidents will be logged by ECMAT as follows:

- General incidents relating to students mis-use, damaged or stolen equipment will be logged on individual pupils' files. Dependant on the seriousness of the incident the matter will be recorded and referred at an appropriate level of seniority, through the e-safety co-ordinator. A full report of all incidents can be extracted at any point.

- Very serious e-safety issues relating to child protection, soliciting, grooming, family issues will be logged in the Child Protection Log and is accessible through **(insert name of Child protection co-ordinator).**The matter should also be communicated to the ECMAT Academies Director and HR Director, and consideration should be given to the matter being reported through to the relevant Local Authority Designated Officer (details available on the ECMAT website).

- E-Safety incidents relating to staff will be dealt with directly by the Headteacher. Appropriate information may be recorded on individual staff files after consultation with the member's trade union.

16.3. Misuse and Infringements

Complaints

Complaints or issues relating to e-Safety should be made to the SIRO, IAO, e-Safety co-ordinator or Headteacher.

The **Becta Flowchart for Managing an E-Safety Incident** given below is a useful referral tool to understand both the severity and processes to be followed.

Inappropriate Material

- All users will be made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator, who will decide – in the case of staff, after consultation with the member's trade union - on the appropriate course of action.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ ECMAT, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

- Users will be made aware of sanctions relating to the misuse or misconduct through the Induction programme.

16.4. Flowcharts for Managing an E-Safety Incident

The course of action would normally follow the left or right hand flowchart. However, If the right hand is followed and the police or relevant authority find no illegal activity an internal review following the left hand chart would take place to ensure the correct outcome for all parties is ensured. Where an alleged incident involves a member of staff, the relevant trade union will be involved throughout this process.

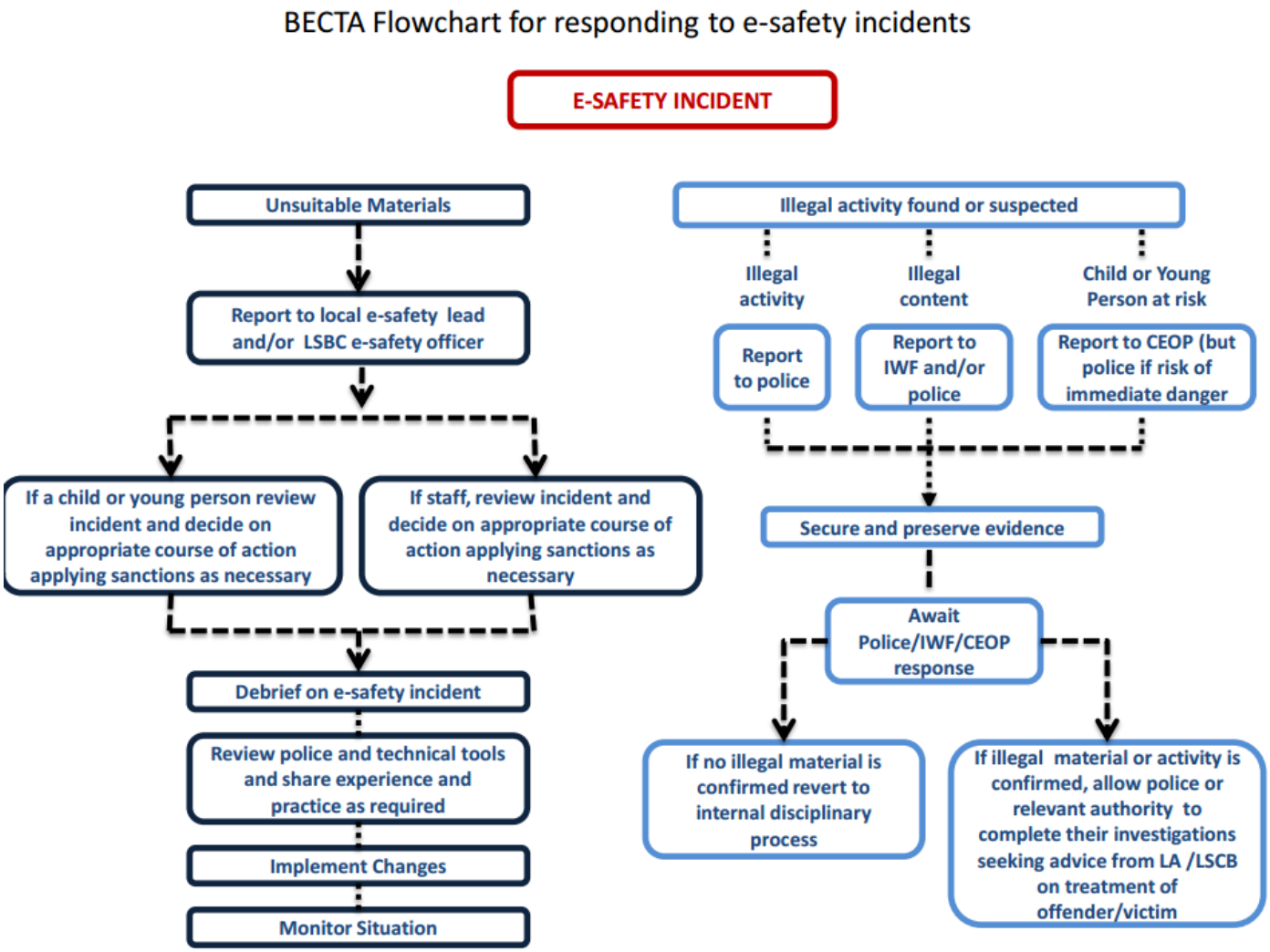
Shortened Terms used

LSBC - Local Safeguarding Children's Board

IWF- Internet Watch Foundation

CEOP - Child Exploitation and online Protection

LA - Local Authority



17. Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

17.1. Managing the Internet

- ECMAT maintains students who will have supervised access to Internet resources (where reasonable) through the local Academy's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute Academy software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

17.2. Internet Use

- Personal, sensitive, confidential or classified information should not be disseminated in any way that may compromise its intended restricted audience
- ECMAT employees should be careful not to reveal names of colleagues, customers or clients or any other confidential information acquired through the course of work on any social networking site or blog
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion on what internet activities are permissible for pupils and how this is disseminated.

Staff internet access will not be unreasonably restricted outside of working hours but the Headteacher retains ultimate discretion over what internet activities are permissible.

17.3. Infrastructure

- The Academy also employs some additional web filtering which is the responsibility of **(insert names and locations or create annex for this purpose).**
- ECMAT is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998

- Staff and pupils will be made aware that ECMAT based email and internet activity can be monitored and explored further if required

- ECMAT does not allow pupils access to internet logs

- ECMAT uses management control tools for controlling and monitoring workstations

- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate

- It is the responsibility of ECMAT, by delegation to the network manager/ICT Coordinator, to ensure that Anti-virus protection is installed and kept up-to-date on all local Academy machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not ECMAT's responsibility nor the network manager's to install or maintain virus protection on personal systems

- Pupils and staff are not permitted to download programs or files on ECMAT based technologies without seeking prior permission from the Headteacher or ICT Manager. If there are any issues related to viruses or anti-virus software, the Headteacher or nominated person should be informed.

18. Managing Other Web Technologies

Other web based technology, including social media and or networking sites (e.g. Facebook, Twitter), if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- Pupils will be are encouraged to be wary about publishing specific and detailed private thoughts online

- Pupils are asked to report any incidents of bullying to their teachers

- Staff may only create blogs, wikis or other media in order to communicate with pupils using systems approved by the Headteacher

- Other than where a member of staff and pupil are related, staff should never have any personal contact with students through social networking sites such as Facebook, Bebo, etc., as this could jepordise a teacher's position of trust and could result in disciplinary action being taken by ECMAT. Any such disciplinary action will involve the member's trade union where the member of staff is being represented.

19. Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting E-Safety both in and outside of the ECMAT family and also to be aware of their responsibilities. To this end ECMAT will make available training on e-safety with parents/ carers and will seek to promote a wide understanding of the benefits related to ICT and associated risks.

- ECMAT will disseminate information to parents relating to E-Safety where appropriate in the form of;
- Information and training courses
- Posters
- Website/ Learning Platform postings
- Newsletter items

20. Passwords and Password Security

20.1. Passwords protocol

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff are required to change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords should be memorable to the user only and be difficult to guess
- User ID and passwords for staff and pupils who have left the Academy are removed from the system as soon as possible to avoid zombie and possible unauthorized access
- Short term cover staff will be given a generic account to allow only basic access

If you think your password may have been compromised or someone else has become aware of your password report this to your Headteacher or Chair of the LAB

20.2. Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends.

All users are required to read and sign an Acceptable Use Agreement to demonstrate that they have understood the ECMAT's e-safety Policy and Data Security

- Users are provided with **(delete/add as appropriate)** an individual network, email, Learning Platform and Management Information System (Staff only) log-in username and initial password. For the network system they are also expected to use a personal password and keep it private
- Pupils are not allowed to deliberately access on-line materials or files from the Academy network, of their peers, teachers or others unless placed on the Learning Platform for their use
- Staff will be made aware of their individual responsibilities to protect the security and confidentiality of ECMAT networks, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- In our Academy, all ICT password policies are the responsibility of **insert name of responsible person** and all staff and pupils are expected to comply with the policies at all times

21. Personal Information Promise

The Information Commissioner's Office launched a Personal Information Promise in January 2009, which all ECMAT are asked to abide by. The personal information promise is: We promise that we will:

1) value the personal information entrusted to us and make sure we respect that trust;

2) go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;

3) consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;

4) be open with individuals about how we use their information and who we give it to;

5) make it easy for individuals to access and correct their personal information;

6) keep personal information to the minimum necessary and delete it when we no longer need it;

7) have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;

8) provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;

9) put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and

10) regularly check that we are living up to our promises on Personal or Sensitive Information

21.1. Protecting Personal, Sensitive, Confidential and Classified Information

- Users should ensure ECMAT information accessed from PCs or removable media equipment is kept secure
- Users should ensure screens are locked before moving away from work stations during the course of the working day to prevent unauthorised access
- Users should ensure the accuracy of any personal, sensitive, confidential and classified information that are disclosed or shared with others
- Users should ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Users should ensure the security of any personal, sensitive, confidential and classified information contained in documents that are faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-ECMAT environment
- Users should only download personal data from systems only with express line-management authorisation
- Users must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Users should be careful to keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information
- Users should ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

21.2. Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Users should Store all removable media securely
- Users should Securely dispose of removable media that may hold personal data
- Users should encrypt all files containing personal, sensitive, confidential or classified data
- Users should ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

- All necessary facilities and training for the above will be provided by ECMAT

22. Remote Access

- Users are responsible for all activity conducted via the remote access facility
- Staff should use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to Academy systems, users should keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and not disclose them to anyone
- Users should select PINs to ensure that they are not easily guessed, e.g. house or telephone numbers or consecutive or repeated numbers are unsuitable
- Users should avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Users should protect ECMAT information and data at all times, including any printed material produced while using the remote access facility. Particular care should be taken when access is from a non- ECMAT environment

23. Safe Use of Images

23.1. Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the Academy community or public, without first seeking consent and considering the appropriateness

- With the written consent of parents (on behalf of pupils) and staff, ECMAT permits the appropriate taking of images by staff and pupils with ECMAT equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips, unless they have their permission
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips unless they have permission.

23.2. Consent of Adults Who Work at ECMAT

- Permission to use images of all staff who work at an ECMAT site is sought on induction and a copy is located in the personnel file

23.3. Publishing Pupil's Images and Work

On a child's entry to an ECMAT Academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the Academy web site
- on the Academy's Learning Platform
- in the Academy prospectus and other printed publications that the Academy may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the Academy's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the Academy
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this Academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. A record of permissions is held by the Academy and will be updated yearly in September

- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Where this is the case i.e. parental newsletters, these will be accessible through the VLE and individual usernames and passwords
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.
- Only the following individuals have the authority to upload to the site **(insert name/s here).**
- ECMAT will ensure that the above process can be done efficiently so as not to increase staff workload.

23.4. Storage of Images

- Images/ films of children are stored on the Academy's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher or Senior Leadership Team
- Any face pictures/images of children at the Academy must not be manipulated without the prior consent of the Headteacher
- Rights of access to this material are restricted to the teaching staff within the confines of the Academy network and pupils within the confines of the Academy network and Learning Platform
- **Insert names of individuals with responsibility** has the responsibility of deleting the images when they are no longer required, or the pupil has left the Academy

23.5. Webcams and CCTV

- On certain Academy sites, ECMAT uses CCTV for security and safety. The only people with access to this are the **Senior Leadership Team and the IAO**. Notification of CCTV use is displayed at the front of the Academy.
- ECMAT does not use publicly accessible webcams
- Webcams in an ECMAT Academy site are only ever used for specific learning purposes, i.e. Skype calls to partner Academy's and are set up for purpose
- Misuse of the webcam by any member of the Academy community may result in sanctions (as listed under the ' inappropriate materials' section of this document)

23.6. Video Conferencing
(delete this section if not appropriate to the Academy and amend contents page)

- All pupils will be supervised by a member of staff when video conferencing with end-points beyond or within an ECMAT Academy site.
- An ECMAT Academy may keep a record of video conferences, including date, time and staff
- Approval from A Senior Leadership Team member is sought prior to all video conferences and is always set up and verified by the IAO
- ECMAT conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

23.7. Additional points for reference:

- Participants in conferences offered by third party organisations may not be DRB checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

24. ECMAT/Academy ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

24.1. Academy ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the ECMAT ICT equipment provided to you
- ECMAT logs ICT equipment issued to staff and records serial numbers as part of the Academy's inventory
- Visitors to the Academy wishing to plug their ICT hardware into the ECMAT network points will only be allowed to do so if this has been checked and cleared or special provision has been made.
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorized access or make unauthorized modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- Important data about students would normally be entered in the ECMAT management system. However, other data, for example on going controlled assessment data should be saved on a frequent basis to the ECMAT's network drive. You are responsible for the backup and restoration of any of your data that is not held on the ECMAT network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- A time locking screensaver should be applied to all machines
- Privately owned ICT equipment should not be used on an Academy network
- On termination of employment, resignation or transfer, all ICT equipment will be returned to the Academy. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be verified through **(insert name of relevant person)** he/she will be are responsible for:

- maintaining control of the allocation and transfer of equipment
- recovering equipment, with the aid of the curriculum line managers, when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

24.2. Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on ECMAT systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all ECMAT data is stored on ECMAT's network, and not kept solely on their laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data with the central ECMAT network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the SIRO, fully licensed and only carried out by relevant parties
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

24.3. Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of the Academy too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in Academy is allowed. Currently ECMAT chooses to manage the use of these devices in the following ways so that users exploit them appropriately. However, the speed of change in this area means that this area needs to be reviewed regularly.

24.3.1. Personal Mobile Devices (including phones)

- ECMAT allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does ECMAT want a member of staff to contact a pupil or parent/carer using their personal device
- Pupils currently are not or are **(delete as appropriate)** restricted from bringing mobile phones to the Academy but are allowed to bring other devices such as ipods **(add/delete as appropriate)** but must not use them for personal purposes within lesson time unless agreed by the teacher to support learning
- ECMAT is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text or internet messages between any member of the ECMAT community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices
- Users bringing personal devices into any ECMAT building must ensure there is no inappropriate or illegal content on the device

24.3.2. ECMAT Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the ECMAT community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the ECMAT community
- Where ECAMT provides mobile technologies such as phones, laptops and PDAs, cameras or videoing equipment for offsite visits and trips, only these devices should be used
- Report the loss or theft of any ECMAT mobile phone equipment immediately to (insert name or job title)
- Where ECMAT provides a laptop for staff, only this device may be used to conduct Academy business outside of Academy
- All ECMAT mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default
- You must not send text messages to premium rate services
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

24.4. Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 21.2 - ‘Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media’ - page 33

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely.

25. Servers

- Servers must be in a locked and secure environment
- Access rights will be limited
- The servers will be password protected and locked
- Existing servers have security software installed appropriate to the machine's specification
- Backup tapes are to be encrypted by appropriate software
- Data is backed up regularly
- Backup tapes/discs should be securely stored in a fireproof container
- Back up media stored off-site must be secure

26. Smile and Stay Safe Poster

and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or name of the Academy. Never reply to ASL (age, sex, location).

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

27. Systems and Access

- You are responsible for all activity on Academy systems carried out under any access/account rights assigned to you, whether accessed via Academy ICT equipment or your own PC

- Do not allow any un-authorised person to use ECMAT ICT facilities and services that have been provided to you

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent un-authorised access

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from ECMAT ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to ECMAT or may bring ECMAT into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the ECMAT's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Equality Act 2010)

- Any information held on ECMAT systems, hardware or used in relation to ECMAT business may be subject to The Freedom of Information Act

- Where necessary, permission will be obtained from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data. If this is done internally then a log is kept ensuring that this action has been taken.

28. Telephone Services

- You may make or receive personal telephone calls provided:

1) They are infrequent, kept as brief as possible and do not cause annoyance to others.
2) They are not for profit or to premium rate services
3) They conform to this and other relevant ECMAT policies
4) ECMAT telephones are provided specifically for ECMAT business purposes and personal usage is a privilege that will be withdrawn if abused. For example: overseas personal telephone calls

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that your incoming telephone calls can be handled at all times
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat or other serious incident warning (See policy relating to The Major Incident Plan).

29. Writing and Reviewing this Policy

Writing

- This policy has been created in conjunction with the Police, IT specialist, Schools and HR, recognized trade unions and the Senior Leadership Team at ECMAT.

Review Procedure

There will be an on-going opportunity for staff to discuss with the SIRO, IAO any issue of data security that concerns them

This policy will be reviewed annually and consideration given to the implications for future whole ECMAT development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way and reviewed in 2016.

30. Current Legislation

Acts Relating to Monitoring of Staff E-Mail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to Academy activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to E-Safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with who they are in a position of trust. Academies should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Appendix 1 - Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in ECMAT. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any breaches will lead to disciplinary action.

I will only use ECMAT's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Local Advisory Board (LAB).

- I will comply with the ICT system security and not disclose any passwords provided to me by the ECMAT or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system for any ECMAT business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in Academy, taken off the Academy premises or accessed remotely. Personal data can only be taken out of Academy or accessed remotely when authorised by the Headteacher or LAB. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory within my Academy role.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in-line with Academy or ECMAT policy. Images will not be distributed outside the Academy network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the ECMAT approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the ECMAT Family or wider community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity and use of other technologies will not bring my professional position of trust into disrepute.
- I will support and promote the ECMAT's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

- I agree to ECMAT using digital photographs/images of myself for security purposes within ECMAT

User Signature

I have had explained the implications of ECMAT's e- safety policy with regard to my code of conduct, supporting the safe and secure use of ICT throughout ECMAT and to the use of digital images. I agree to follow this agreement

Signature …… Date ……..……

Full Name …….....(printed)

Job title ……