Trust E-Safety Policy
V3.9

Date:	17.04.18
Date reviewed by policy committee:	

Date approved by policy committee:	09.05.18
Responsible for this policy:	Trust ICT Lead

Approval History

Approved By:	Date of Approval	Version Approved	Comments
Policy Committee		V1.0	
Policy Committee	11.09.15	V3.6	
Policy Committee	20.07.16	V.3.8	
Policy Committee	09.05.18	V3.9	

Revision History

Revision Date	Previous Revision Date	Rev	Summary of Changes	Changes Marked	Owner/Editor
24.04.15		V3	CWR changes made to include both schools	Yes	CWR
30.04.15		V3.1	Updated as per academy template. Updated Page numbers Inserted footers and dated. Changed pupil to student. Changes made to contents page. Changes made as per governor meeting on the 02.04.15	Yes	WBE
05.05.15		V3.2	Added appendix 3 and 4.	Yes	WBE
15.06.15		V3.3	P11 bring your own device insertion of *(on school grounds or if being used for a work related activity) and two principles of unacceptable use.* P12 *insertion of Director of Learning bullet point f* P18 *insertion of Appendix 2 on use of the Internet and e-mail*	Yes	WBE/CWR
02.07.15		V3.4	Changes made after union consultation	Yes	WBE
06.07.15		V3.5	Replace Business Manager name with Dr J MacKinnon page 4.	Yes	WBE
11.09.15		V3.6			KLU
21.09.15		V3.7	Added the phrase 'extreme or radicalising' to the definitions and online behaviours p9,10 and 19	Yes	CWR

Revision Date	Previous Revision Date	Rev	Summary of Changes	Changes Marked	Owner/Editor
04.07.16		V3.8	Replaced the word virus/worm with malware – paragraph 3.3, p.6 Inserted the words unauthorised and audio files – paragraph 3.4, p.7 Replaced Directors of Learning with Progress Leaders – paragraph 4.0, p.8, p.9 Inserted reference to the visitor policy under images and videos – paragraph 6.0, p.11 Replaced Show My Homework with Doddle – paragraph 6.0, p11 Inserted the words living or identifiable under paragraph 11.0 – data protection, p.14. Appendix 1 - Additional text inserted regarding taking care of portable equipment, use of the internet and e-mail, the use of social networking sites, use of webcams, refusal of invitations from current students to take part in on-line gaming forums.	Yes	CWR/SME
17/04/2018		3.9	Changes of names in key personnel		
17/04/2018		3.9	Inserted reference to centralised software register – paragraph 6, p11		
17/04/2018		3.9	Remove paragraph on Data protection – paragraph 8, p11		
17/04/2018		3.9	Additional paragraph relating to BYOD – Any device that will be used to access Trust data must be encrypted and be secured with a password or PIN. The member of staff must undertake that this device will never be shared with another person whilst those services are logged in and available to prevent accidental disclosure of data. - paragraph 1, p.12		
17/04/2018		3.9	Changed the text ‘Section 7’ to ‘Data protection policy – paragraph 2, p.12		

17/04/2018		3.9	Remove section 7 – p.12 and renumber subsequent paragraphs accordingly		
17/04/2018		3.9	Remove section 11 – p.15 and 16 and renumber subsequent paragraphs accordingly		
17/04/2018		3.9	Re-phrasing from 'personal mobile phone' to 'personal connection to the Internet' – Paragraph 2, Bullet point 6, p.19		
17/04/2018		3.9	Change Data Protection Act to General Data Protection Regulation – paragraph 1, bullet point 7, p.20		
17/04/2018		3.9	Change Section 7 to Social Media Policy – paragraph 1, bullet point 8, p.21		
17/04/2018		3.9	Addition of the word trust to reflect the cross-trust nature of the web developers role – paragraph 3, bullet 1, p.21		
17/04/2018		3.9	Change of the term 'Learning gateway to 'Remote Desktop' to reflect change in technology used. Paragraph 3 p.22		
17/04/2018		3.9	Change of bullet points to reflect the use of this alternative technology. Paragraph 3, p.22		
17/04/2018		3.9	Remove appendix 4 – no longer valid technology		

CONTENTS

1. Purpose of the Policy 6
2. Roles and Responsibilities 6
3. IT User Responsibilities 7
4. Reporting 8
5. Acceptable and Unacceptable use 11
6. Equipment and Services 11
7. Communication and Social Contact 13
8. Access to inappropriate images 13
9. Cyberbullying 14

10.Appendix 1 – Education and Leadership Trust Procedures 15
11.Appendix 2 – IT User responsibilities 21
12. Appendix 3 – Device Responsibility 22

1.0 PURPOSE OF THE POLICY

This policy defines and describes the acceptable use of IT for staff and students at the Education and Leadership Trust (ELT). Its purpose is to encourage the creative use of technology to engage learners, minimise the risks to students of inappropriate situations and materials, protect the staff and school from litigation and to minimise the risk to the IT network and systems.

This policy deals with the use of IT facilities and associated web-based services across the Trust and applies to all school employees, students and authorised users.

This policy must be read in conjunction with the Child Protection Policy, the Behaviour Policy, the use of Social Media Policy, the Data Protection Policy and the Freedom of Information Policy.

2.0 ROLES AND RESPONSIBILITIES

The Trust Board is responsible for ensuring that its employees, governors and Trust directors act in a lawful manner, making appropriate use of school technologies for approved purposes only.

The Local Governing Body is responsible for implementing relevant policies and the Academy Headteacher is responsible for ensuring that staff are aware of their contents.

The Academy Headteacher is responsible for maintaining an inventory of IT equipment as part of the school asset management register and recording to whom it has been issued.

If the Academy Headteacher or Executive Headteacher has reason to believe that any IT equipment has been misused by an adult, they will consult the Trust's HR provider for advice without delay. The HR provider will agree with the Academy Headteacher or Executive Headteacher an appropriate strategy for the investigation of the allegations and liaison with other agencies as appropriate. Incidents will be investigated in a timely manner in accordance with agreed procedures. The Academy Headteacher and Executive Headteacher will make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

It is also important to recognise that esafety is not an IT issue. It may involve the use of IT, but it is about protecting children and young people from harm. If you have a concern about actual, significant harm to a child or young person, or the risk of significant harm, then you should make immediate contact with the Child Protection Officers in school.

Key personnel	Whalley Range	Levenshulme	TEMA
e-safety Lead	Mrs Catherine Wragg	Mrs Catherine Wragg	Mrs Catherine Wragg
Data Controller	Ms Debbie Collier	Ms Debbie Collier	Ms Debbie Collier
Lead Child Protection Officer	Mrs Jackie Fahey	Ms Donna Johnson	Mr Martin Birrell

3.0 IT USER RESPONSIBILITIES

Use of Education and Leadership Trust IT resources is granted based on acceptance of the following specific responsibilities:

I. Use only those computing and information technology resources for which you have authorisation.

For example: it is a violation

- to use resources you have not been specifically authorised to use
- to use someone else's account and password or share your account and password with someone else
- to access files, data or processes without authorisation
- to purposely look for or exploit security flaws to gain system or data access

II. Use computing and information technology resources only for their intended purpose.

For example: it is a violation

- to send forged email or other electronic communication
- to misuse Internet Relay Chat (IRC) software to allow users to hide their identity, or to interfere with other systems or users
- to use electronic resources for harassment or stalking other individuals
- to send chain letters, bomb threats or "hoax messages"
- to intercept or monitor any network communications not intended for you
- to use computing or network resources for advertising or other commercial purposes
- to use electronic resources for personal use at inappropriate times or in inappropriate locations
- to attempt to circumvent security mechanisms

III. Protect the access and integrity of computing and information technology resources.

For example: it is a violation

- to intentionally release any malware that damages or harms a system or network
- to prevent others from accessing an authorised service
- to send email bombs that may cause problems and disrupt service for other users
- to attempt to deliberately degrade performance or deny service
- to corrupt or misuse information
- to alter or destroy information without authorisation

IV. Abide by applicable laws and school policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.

For example: it is a violation

- to make unauthorised copies of licensed software
- to download, use or distribute pirated software
- to upload or download pirated copies of video or audio files
- to operate or participate in pyramid schemes
- to upload, download or distribute inappropriate material

V. Respect the privacy and personal rights of others.

For example: it is a violation

- to tap a phone line or run a network sniffer without authorisation
- to use photographs of individuals, for Trust purposes, without permission
- to access or attempt to access another individual's password or data without explicit authorisation from a senior member of staff, with the direct knowledge of the Academy Headteacher or Executive Headteacher.

All staff will be required to sign an agreement each September (or on starting if during a school year) to indicate that they have read and understood these responsibilities. (See Appendix 2) The signed copy will be kept with the e-safety coordinator.

4.0 REPORTING

Staff are responsible for reporting every breach of esafety. If a member of staff knows, or suspects, that a colleague is in breach of any part of this policy he/she must report it to the appropriate person in writing by email to the following leads and copy in the Academy Headteacher.

Immediate reporting:

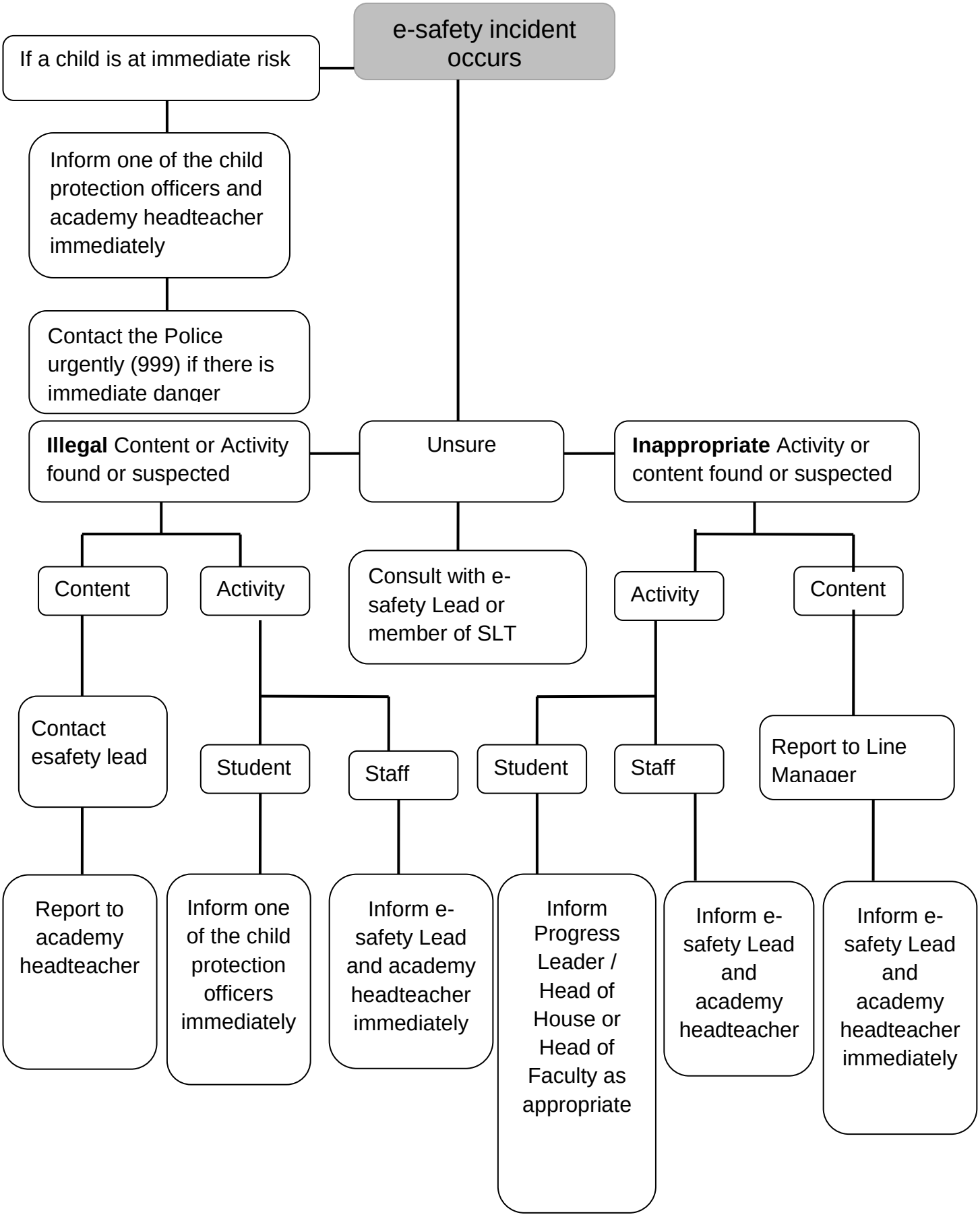
Child protection incident	– to Child Protection Officers
Illegal Activity or Material	– to e-safety Lead
Inappropriate activity by a member of staff	– to e-safety Lead
Illegal content or material which requires immediate removal or blocking	– to onsite technicians and e-safety Lead

Same day reporting:

Inappropriate material which requires additional filtering on the Internet	– to onsite technicians and e-safety Lead
Inappropriate activity by a student in a lesson (which does not	– to Heads of Faculty/Subject

constitute a child protection incident)	
Inappropriate activity by a student not in a lesson (which does not constitute a child protection incident)	– to Heads of House / Progress Leaders

Staff are required to be vigilant when students are using computers. Students accessing inappropriate materials must be reprimanded and repeated offences must be reported using the school behaviour systems.


e-safety incident occurs
If a child is at immediate risk
Inform one of the child protection officers and academy headteacher immediately
Contact the Police urgently (999) if there is immediate danger
Illegal Content or Activity found or suspected
Unsure
Inappropriate Activity or content found or suspected
Content
Activity
Consult with e-safety Lead or member of SLT
Activity
Content
Contact esafety lead
Student
Staff
Student
Staff
Report to Line Manager
Report to academy headteacher
Inform one of the child protection officers immediately
Inform e-safety Lead and academy headteacher immediately
Inform Progress Leader / Head of House or Head of Faculty as appropriate
Inform e-safety Lead and academy headteacher
Inform e-safety Lead and academy headteacher immediately

5.0 ACCEPTABLE AND UNACCEPTABLE USE

The rapid developments in hardware and software mean that use of technology changes at an unprecedented rate. It would be impossible to document every potential use of IT equipment in school.

Within the ELT, we believe that the use of technology is an essential part of education in the 21st century. Young people are immersed in a digital world where information is available 24 hours a day, 7 days a week. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can be used to encourage discussion, provide outlets for creativity and enrich the curriculum. The use of e-mail, mobile phones, Internet messaging and blogs all enable improved communication on an unprecedented scale and our Virtual Learning Environment will offer a platform for personalised and independent learning, twenty four hours a day.

In addition to these benefits, however, there are risks and unfortunately some young people may expose themselves to danger either knowingly or unknowingly. Staff and students may inadvertently come across unsavoury, distressing or offensive materials on the Internet and some social networking sites offer cover for unscrupulous individuals to groom children. It is crucial that whilst promoting the positive use of technology in our school, we recognise the potential risks and take steps to protect our students, staff and visitors.

Instead the incorrect use of IT within the Education and Leadership Trust is underpinned by the term 'Unacceptable Use'.

Unacceptable Use is defined as any activity which is; conducted without permission, outside the specific learning aim for that lesson or activity, illegal, considered extreme or radicalising, dangerous or where the equipment is used to make any student, member of staff or member of the public feel uncomfortable or vulnerable.

Acceptable use is therefore taken to mean the use of the resources to; create imaginative learning opportunities, efficient business practice, continuing professional development and other uses which enable staff and governors to maintain a healthy work-life balance.

6.0 EQUIPMENT AND SERVICES SUMMARY

IT Equipment – the term relates to any equipment provided by school including computers, portable devices and phones.

Any equipment must be used with care and take precautions to ensure it is left ready for other users when finished. Damaged, broken or missing equipment must be reported immediately to the relevant person.

Network logon and password – All users are issued with a user name and password with access rights tailored for their use of the IT systems in school provided they accept the responsibilities outlined in Appendix 2. (IT user responsibilities)

All users must access the network only using their own logon and password. Passwords must not be disclosed or shared. The user assumes full responsibility for the use or misuse of this account.

Personal Use – Staff are permitted to use Trust IT equipment for personal use providing it is not in breach of the term 'Unacceptable Use'. All users must use any equipment appropriately and responsibly at all times and assume full responsible for any activity carried out using their account or on equipment being used by them at the time.

Internet Access – A filtered and managed connection to the Internet is provided to all users. Staff and students must not access, or attempt to access websites that contain any of the following: child abuse; pornography; extreme or radicalising views; promotion of discrimination of any kind; promoting illegal acts; any other information which may be illegal or offensive. It is recognised that under certain circumstances inadvertent access may occur. Should staff or a student access any sites which may fall into the categories described above you must report it in accordance with the reporting procedures.

Email – An email account is provided to each member of staff and student. All communications for professional business including contact with students and parents must be done through the school email systems. Any emails sent through the school system must be appropriate and professional.

Monitoring – Internet activity, network activity and email are subject to monitoring and may be viewed without prior warning.

Images and Videos – We encourage staff and students to use IT to capture work and achievements as part of a portfolio of evidence or to celebrate work or achievements. No images or videos should be uploaded to any website or social network without permission and in the case of students, this includes the permission of the parents/carers. No images or videos of students should ever be uploaded to staff personal websites or social network accounts. For images and videos with visitors, please see the visitor policy

External Services and Systems – We use a range of services provided by third parties such as Frog, Office 365 and Doddle which provide valuable resources to all members of the Trust. Users must only log into these services using their own login and password. Users are responsible for all activity carried out during a session using your login. A centralised register of these systems exists and is visible through the VLE. Users may not create accounts for staff or students on systems which are not on the list.

Copyright including Software licensing – The school provides all users with access to a range of software and services which are licensed by agreements with the companies involved. Only licensed copies of software may be installed on any device. Users may not download copyrighted software, audio or video files or any other copyrighted material. Any such material found will be deleted without prior notification.

Bring Your Own Device (BYOD) – Staff are permitted to use their own personal IT equipment in school at the discretion of the Academy Headteacher. The use of any personal device on school grounds or if being used for a work related activity is subject to the same principles of 'unacceptable' use as any device owned by the school or the Trust.

Any device that will be used to access Trust data must be encrypted and be secured with a password or PIN. The member of staff must undertake that this device will never be shared with another person whilst those services are logged in and available to prevent accidental disclosure of data.

It is the responsibility of the member of staff to ensure that any device brought into school by them is used appropriately and within the scope of this policy. The member of staff is responsible for any use or misuse of this device whilst it is on school grounds or if it is being

used for a work related activity. You are responsible for ensuring that any use adheres to the Data Protection procedures outlined in the Data Protection policy.

The Education and Leadership Trust IT Appendices – These documents cover day to day operation and procedures in more detail and will be made available to all staff as appendices to this policy. Procedures will be reviewed annually and may slightly differ between individual schools.

7.0 COMMUNICATIONS AND SOCIAL CONTACT

a) Adults should keep their personal phone numbers, work login or passwords and personal email addresses private and secure. Where there is a need to contact students or parents a school system should be used e.g. telephone, email or messaging service.
b) Adults must understand who is allowed to view the content on their pages of any sites they use and how to restrict access to certain groups of people.
c) Communication between students and adults by whatever method, must take place within clear and explicit professional boundaries. Staff should use their school email for all contact with students.
d) Adults must not request, or respond to, any personal information from a student.
e) Adults must ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with students in order to avoid any possible misinterpretation of their motives or any behaviour which could possibly be construed as 'grooming' in the context of sexual offending.
f) E-mail or text communications between an adult and a student outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems must only be used in accordance with the school's policy.
g) There may be occasions when there are social contacts between students and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged with the Headteacher where there may be implications for the adult and their position within the school setting.
h) There must be awareness on the part of those working with or in contact with students that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the adult's own family.
i) Any concerns must be raised with the Headteacher at the earliest opportunity.

8.0 ACCESS TO INAPPROPRIATE IMAGES

a) There are no circumstances that justify adults possessing indecent images of children. Staff who access and/or possess links to such material or websites will be viewed as a significant and potential threat to children. This will lead to criminal investigation and disciplinary action. Where indecent images of children are found, the Headteacher must be informed immediately.
b) Adults must not use equipment belonging to the school to access any adult pornography or any inappropriate images; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.
c) Adults should ensure that students are not exposed to any inappropriate images or web links. The school endeavours to ensure that internet equipment used by students has the appropriate controls with regards to access. e.g. personal passwords should be kept

confidential. Any potential issues identified must be reported to the e-safety lead immediately.

d) Where other unsuitable material is found, which may not be illegal but which could or does raise concerns about a member of staff, advice should be sought from the e-safety lead before any investigation is conducted.

9.0 CYBERBULLYING

a) Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

b) If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Staff are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

c) Staff are encouraged to report any and all incidents of cyberbullying to their line manager or the Academy Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police. Staff may wish to seek the support of their trade union or professional association representatives.

APPENDIX 1

10.0 USE OF THE ACADEMY HARDWARE AND NETWORK (via any wired or wireless device):

- Staff must sign the 'IT User Responsibilities' agreement before access to the network is permitted.
- Users shall not in any way, tamper or misuse academy equipment, either software or hardware.
- Users must only access the network using their own logons and passwords. These must not be disclosed or shared.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- The user takes full responsibility for the use or misuse of this account.
- Software, including apps should not be installed without proper licensing arrangements.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.
- Users must not make any attempt to remove, replace or disable the anti-virus software installed on any academy device.
- Staff must logout of SIMS when leaving a classroom for any period of time.
- Access to storage areas on the network is permitted on an individual needs basis and will be determined by the Academy Headteacher.
- Staff must only place material for professional or educational purposes on the shared areas of the network.
- Staff are responsible for removing material which is no longer relevant.
- Devices in either academy can have access to the Internet. Abuse of this access, in the form of access to pornographic sites is absolutely forbidden. Please note that access to certain pornographic sites may be in serious breach of the law (Child Trafficking and Pornography Act 1998). The academy will fully co-operate with the relevant authorities in investigating and prosecuting any such illegal access.
- The ICT facilities are for Academy related educational use and personal use only. The ICT facilities are not available for use on external projects or for work or business activities not associated directly with courses or the Academy. ICT facilities may not be used for any form of personal financial gain. Exam marking is acceptable.
- The contents of all mailboxes, PCs, server shares, cloud storage areas and caches operated by the Academy, remain the property of the Academy. The status of these data stores is similar to that of letters posted to the Academy to a post holder (not marked as personal and private).
- Notwithstanding that every effort is made to ensure that home folders and e-mail are secure, the Academy does not in any way guarantee the security of this data.
- Food and drinks should be kept well away from ICT equipment.
- The user should take care when shutting down and closing the lids of laptops to ensure that nothing is left lying on top of the laptop surface. This may result in damage not covered by warranties, in which case the user will be liable for repair costs.
- The user should take care when moving any portable device, especially iPads. Devices should be securely fastened in their protective cases (where applicable) before moving.

Installing software

- Only licensed software may be installed onto academy owned devices.
- Software in use in the Academy is licensed in a correct and legal manner. However (except where explicitly stated), it is not available to users for home usage. Users should make no attempt to copy licensed or copyrighted material from the Academy network.
- Teachers are not authorised to install unlicensed software on any device. If a member of staff requires special or non-standard software to be installed on any device, it must be licensed in a correct and legal manner. The member of staff will be responsible for supplying licenses, media, and any documentation on request if not purchased through the IT budgets.
- Users may not download copyrighted software, audio or video files, or any other copyrighted material from the Internet. Any such material found will be deleted without prior notification.
- Breach of these conditions may lead to disciplinary action.

Use of mobile phones and other mobile devices

- Staff are required to switch mobile phones to silent during lessons, assemblies and other academy based events.
- The taking of still pictures or video footage without the subject's permission is not ethical, and staff must ensure that any images captured for educational purposes are treated in accordance with the rules set out in the section referring to cameras.
- Any person recording any image for malicious purposes will be subject to disciplinary procedures.
- Students and staff are encouraged to report malicious texts or phone calls to the appropriate authority (including teaching staff and the academy-based police officer)
- Staff and students are discouraged in their use of a personal connection to the Internet on a mobile phone during academy time and on academy property as this by-passes the security systems set in place to protect individuals.
- For the use of mobile devices in relation to visitors, please refer to the visitor policy.

Use of Personal ICT equipment in academy

- Staff must not bring any item of equipment onto the academy premises which contains materials which directly contravene the e-safety policy. This may include e.g. inappropriate photographs or illegal copies of software.
- Any item which requires mains power, and which will be plugged into the academy's electricity supply, must be Portal Appliance Tested (PAT) prior to use. Staff must take the appliance to the Facilities Office where they will arrange for the equipment to be tested.
- Staff may connect their own devices to the wireless network in either academy. All access to the Internet must be conducted using their own login and password and all Internet traffic is subject to filtering and monitoring.

Use of the Internet and e-mail:

- Staff must sign the 'IT User Responsibilities' agreements before access to the internet and email is permitted.
- Staff may only send e-mails to students using the academy e-mail system.
- Staff must not open e-mails sent from a current student's personal e-mail account unless there is specific permission from the academy headteacher e.g. in the case of exams officers sending results to students.
- If a member of staff is sent an e-mail by an ex student, they should only use the academy e-mail system to respond.

- Users must access the Internet and e-mail using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's e-mail account.
- The Internet and e-mail should primarily be used for professional and educational purposes. Personal use of the Internet is permitted provided it does not breach the term 'Unacceptable Use', does not contravene any other policy of the Trust or academy and is carried out at appropriate times. Personal use of the Internet at inappropriate times or that breaches any other school or Trust policies may be subject to disciplinary procedures.
- All users must respect the need for Internet filtering and not deliberately try to by-pass the security systems.
- Students must be supervised at all times when using the Internet and e-mail in a learning situation.
- Accidental access to inappropriate, extreme or radicalising, abusive or racist material must be reported without delay to the on-site technicians and e-Safety Lead and a note of the offending website address (URL) taken so that it can be blocked.
- Internet and e-mail filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence.
- Internet and e-mail use will be monitored regularly in accordance with the General Data Protection Regulation
- All Internet account histories and academy e-mail accounts are accessible to the eSafety Lead and may be checked without prior consultation.
- Users must not disclose any information of a personal nature in an e-mail or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All e-mails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Usage of any form of profanity in these communications is absolutely forbidden. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- All e-mails sent from an establishment/service e-mail account will carry a standard disclaimer disassociating the establishment/service and the Local Authority with the views expressed therein.
- Bullying, harassment or abuse of any kind via e-mail will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive e-mails are received, this must be reported immediately to a trusted adult or member of staff within the service / establishment. E-mails received should not be deleted, but kept for investigation purposes.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.
- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.
- E-mail should be considered as an insecure medium for the transmission of confidential information. Where confidential information is to be transferred, in particular externally, it should be done in an encrypted form.

Use of Chat and Weblogs during lessons

- Use of social-networking websites (e.g. Facebook, Twitter, Snapchat etc.) is not permitted during lessons unless the site is being accessed to make a specific educational point.
- Students and staff must not access public or unregulated chat rooms.

Use of Social Networking Sites

- Social networking sites are unblocked for staff but should only be accessed at appropriate times.
- Staff using such sites outside of academy should not add current students as friends or contacts or use the site to contact current students. If staff do already have students as contacts, they are advised to delete these contacts with immediate effect.
- Staff are discouraged from adding ex-students as contacts as many of them have current students as friends and information can be disclosed to current students through these links.
- Staff should not put photographs of current students on any social networking site.
- Staff should ask for permission before putting photographs of other staff on any social networking site.
- Staff are advised not to add personal details to their social network sites for their own safety.
- Staff must not put personal details of their colleagues or students on their social network sites.
- Professional social media accounts are permitted providing the user follows the guidelines in Social Media Policy

Use of Cameras, Video Equipment and Webcams

- All parents are notified of the academy's policy on its use of student photographs and other media. A record of any response is kept up to date in SIMS.
- Photographs or video footage must be downloaded immediately and saved into a designated folder.
- Any photographs or video footage stored must be deleted immediately once no longer needed.
- Any adult using their own camera, video recorder or camera phone during a trip or visit must transfer and save images and video footage into a folder in a staff shared area of the network, at the earliest opportunity and delete the images from their own device.
- Students should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do, and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straightaway.
- Video conferencing equipment and webcams must be switched off (disconnected) when not in use.
- Webcams must not be used for personal communication and should only be used by students with an adult present and with written consent from parents/carers.
- Students and staff must conduct themselves in a polite and respectful manner when representing the establishment/service in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Safety of the Trust and academies websites

- The Trust and each academy has a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published.
- The academy website is subject to frequent checks to ensure that no material has been inadvertently posted, which might put students or staff at risk.
- Copyright and intellectual property rights must be respected.
- Permission will be sought from parents or carers before any images of students can be uploaded onto the academy website.

- Full names should not be used to identify students portrayed in images uploaded onto the academy website, apart from the academy head girl/boy.
- When photographs to be used on the website are saved, names of individuals should not be used as file names.
- Any part of the academy website which contains a Guestbook, public noticeboard, forums or weblogs, will be monitored regularly to check that no personal information or inappropriate or offensive material has been posted.

Using portable games consoles and media players

- The use of portable games consoles and media players for students is only permitted at social times, unless specifically directed by a member of the teaching staff during a particular educational activity.
- Staff are encouraged to take a professional attitude in their own use of portable games consoles and media players in academy time.
- Staff must not arrange to contact current students via on-line gaming forums and must refuse invitations from current students.

Use of Remote Desktop services

- Staff logins and accounts will grant access to remote desktop services via an Internet browser or mobile app.
- Staff must access the remote desktop only using their own logons and passwords. These must not be disclosed or shared.
- Staff must respect confidentiality and attempts should not be made to access another individual's account without permission.
- Staff must take care not to accidentally disclose personal information via accidental public view of a computer screen or by leaving themselves logged in to a device where other users can access the service without further login.
- All users are required to undertake a visual check of their surroundings before logging onto the remote desktop from a computer in a public space, to ensure complete privacy.

Using laptops, chromebooks, i-pads and other devices in school

- Staff must book devices for use in lessons in accordance with the academy mechanisms.
- Staff must conduct a visual check of equipment at the start of the session.
- All devices in a set/trolley must be present and the lights should indicate that they are connected for power and data supply where applicable.
- If a device is missing from a trolley, staff must report this immediately to the onsite technicians who will liaise with the appropriate person responsible for that trolley and the esafety lead.
- Device trolleys must only be moved by members of staff. No students are permitted to move device trolleys. If a member of staff requires help moving the trolley, this should be indicated at the time of booking.
- Staff should conduct a visual check before moving any trolley and should not attempt to move any trolley until it is safe to do so.
- Staff must ensure that trolleys do not block any doorways or fire exits.
- If students request spare devices for other teaching rooms, a member of staff is free to loan the devices to them with the following considerations:
    - Students may only carry one device each
    - The member of staff with the trolley booking is still responsible for the safe return of all equipment at the end of the booking session
- All devices must be returned to the trolley at the end of the booking session, plugged in for power and data where applicable.

- All trolleys must be returned to their base at the end of every school day and the trolley must be plugged in to charge and receive data updates every night.
- When in use, all mobile devices are subject to the same regulations as every other piece of ICT equipment in the building.

APPENDIX 2

11.0 IT USER RESPONSIBILITIES

(Staff initial each line please)

I agree to only use only those computing and information technology resources for which I have authorisation

_____

I agree to only use computing and information technology resources only for their intended purpose.

_____

I agree to protect the access and integrity of computing and information technology resources.

_____

I will abide by applicable laws and school policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.

_____

I will respect the privacy and personal rights of others.

_____

By accepting the IT user responsibilities, you agree:

1. You have read and agree to follow the procedures laid out in the school's esafety policy
2. That you understand that esafety is an important aspect of child protection and you will report any concerns to the relevant staff as per the guidelines
3. That the term 'ICT equipment' applies to any computer, phone or mobile electronic equipment belonging to you or the school
4. You may be subject to disciplinary procedures if found to be in breach of the procedures laid out
5. You will take reasonable steps to ensure that, when using the ICT facilities, all personal data, the school network and the school computer systems are protected from deliberate or accidental damage or disclosure, whether using the system in school or through a remote login
6. To report any breaches of esafety to the relevant person
7. That you understand that you may be subject to legal proceedings if you are in breach of the Data Protection Act or any other legislation in place to protect the individual
8. That you understand that your files and e-mails may be accessed by the Academy Headteacher (or designated person) without my prior consent
9. That you will not attempt to by-pass security systems or make illegal copies of files or software
10. That if you use social media sites, you will maintain a professional presence at all times

Staff Signature Date

APPENDIX 3

12.0 DEVICE RESPONSIBILITY CONTRACT AND CONSENT (Signed on receipt of school device)

Staff Name

I acknowledge receiving a for use while I remain in the employment of The Education and Leadership Trust. I have read the school esafety policy. In order to maintain this privilege, I agree to the following responsibilities:

(Staff initial each line please)

_____ I agree to keep this device in my possession at all times. I will not give or lend it to anyone except to return it to the school for upgrades, network connection or repair in case it is damaged.

_____ I agree not to leave this device on view in my car when it is left unattended.

_____ I agree to carry this device in a padded case or backpack, to minimise the chances that it will be damaged or destroyed.

_____ I agree to read and follow the school's esafety Policy, and will not use this device, in or out of school, for unacceptable or unlawful purposes.

_____ I agree to turn in my device to the school whenever requested for occasional maintenance, updates, or repairs.

_____ I understand that if my device is lost or stolen, I will immediately notify the School.

_____ I agree to return this device to the school before I leave the school

_____ I understand that failure to comply with any of these rules and policies will result in the suspension of my use of this laptop. Restoration of this privilege will require the involvement of the Headteacher.

Staff Signature Date

Checked by Network Manager