ICT AND E-SAFETY POLICY

Including:

Laptop and Mobile Device Policy.

ELT E-safety and LRA Cyberbullying Policy.

ELT Social Networking Policy

Date Published:	**May 2018**
Version:	**V5**
Authors:	**A.Ives/ ELT**
Date shared with Governors:	**May 2018**
Review Date:	**May 2019**
Date shared with Staff:	**May 2018**

ICT CURRICULUM USAGE AND NETWORKING POLICY

PURPOSE AND AIMS

ICT plays a vital part in our lives and it is constantly changing, requiring us to learn and encompass more and more technological information. It provides a powerful communication tool, allowing us to analyse and respond to a wide range of information. It is also recognised as a strong motivating force for children to support the raising of standards across all curriculum areas.

AIMS

- To provided access to ICT opportunities for all children and staff
- To ensure ICT is used across the curriculum and in the wider work of the academy
- To monitor, record and assess children's progress across the curriculum
- To promote safe and responsible use of ICT
- To develop the profile of the academy through the academy website
- To keep pace with developing technology

ROLES AND RESPONSIBILITIES

The ICT technician is responsible for

- Ensuring all hardware and software is working ready for use as far as is possible
- Being available for troubleshooting with IT issues
- Purchasing hardware and all software for academy
- Purchasing curriculum software
- Tracking use of curriculum software
- Ensuring the website is kept up to date and compliant with Ofsted
- Backing up data
- Ensuring web filtering and security maintains the integrity of safeguarding

The ICT Co-ordinator is responsible for:

- Ensuring that policy is best practice, up to date and fit for purpose through monitoring of the policy, its review and update annually.
- Monitoring children's progress within the computing curriculum
- Monitoring the effectiveness and impact of ICT on outcomes and the personal development and well being of staff and students.
- Overseeing the Whizz Kids (digital leaders)
- E-safety committee (as part of H&S, Wellbeing Committee)
- Develop an e-safety culture, act as a named point of contact on all e-safety and promote the e-safety vision to all stakeholders and supporting them in their understanding of the issues
- Ensure that e-safety is embedded within the continuing professional developments for staff and co-ordinate training as appropriate
- Ensure that e-safety is embedded across the curriculum and activities within the organisation as appropriate
- Develop an understanding of the relevant legislation
- Liaise with the trust and other local bodies as appropriate

Staff are responsible for

- Reporting any ICT issues to the ICT technician.
- Ensuring E-safety is of the highest priority.
- Providing high quality integrated computing and ICT learning opportunities for children to apply skills cross curricular subjects
- Planning skills based plans for progression
- Fully complying with this policy
- Ensure that they understand the risks that the students face
- In the event of a disclosure report it using the school's Child Protection and Safeguarding Policy
- Supervision of students at all times when using ICT

The Principal/Head of School is responsible for:

- Ensuring appropriate arrangements are in place to comply with this policy
- Making sure all users are aware of this policy
- Ensuring that appropriate training is undertaken
- Ensuring that the technical infrastructure / network is as sa fe and secure as possible
- Updating the list of inappropriate websites which fall through the filtering software
- Investigation and implementation of discipline matters in relation to this policy.

Governors through the Health, Safety and Well-being committee are responsible for:

- Appropriate budget is allocated to enable the academy to maintain and develop further ICT capability.
- Overseeing the implementation of the ICT policy
- Undertaking the role of the E-safety work group in partnership with the Whizz Kids and parents as appropriate.

CURRICULUM

All children will be given opportunities to:

- develop word processing skills
- develop control of wide range of hardware including tablets, laptops and PCs.
- develop Computer Aided Design skills
- use a range of multimedia software across the curriculum
- use ICT to communicate with others
- simulate and model situations
- store, retrieve and communicate data
- use ICT to create music
- research and find out information
- develop coding and programming
- learn how to be safe online and how to prevent and deal with cyber-bullying
- learn how to ensure that they work safely on ICT equipment e.g. posture and length of time with regards eye-strain.
- incorporate appropriate terminology in their work as well as make good use of ICT learning across the curriculum.
- Manage their own file directories

1. ICT is integrated across the curriculum, to support outstanding teaching, learning and assessment.

2. All staff and children have access to the filtered internet including the use of e-mail as a key communication tool

3. Children are given opportunities to use a range of technology including tablets, data loggers, raspberry pi laptops including Roamers, Beebots, ipads, digital cameras, microphones and interactive whiteboards etc

4. Staff will use ICT in order to inform and enhance their own professional practise.

5. Resources including hardware will be managed and future development will be planned for.

6. Parents/guardians will be asked to sign a consent form for use of images.

7. All students will be asked to complete an Acceptable Use of the Internet form list of children without consent is kept in each classroom and centrally by the admin team.

STAFF COMPUTER SECURITY AND PROTECTION

Each member of staff will be provided with an encrypted personal account for accessing the computer system, with their own username and password. This account will be tailored to the level of access required and will be for that user's use only. As such, users must not disclose password information to anyone, including the ICT Technicians. In the event of a password becoming compromised, users will be required to change their password immediately.

- Passwords will be updated as per protocols decided by the ICT Co-ordinator.
- Personal computers and devices must not, under any circumstance, be used for academy related purposes.
- Members of staff must not allow a student to have individual use of a staff account under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, it must be ensured that the computer is either logged off, or locked to prevent anyone using another's account (press "Win" & "L").
- Users must not store any sensitive or personal information about staff or students on any portable storage system, such as a USB memory stick, portable hard disk or personal computer.
- When publishing or transmitting non-sensitive material outside of the academy, staff must take steps to protect the identity of any student whose parents have requested this.
- Users must ensure that any academy-related sensitive or personal information is secured to prohibit access by any non-member of staff.
- Backups of data kept on any storage system other than the network storage drives should be performed on a regular basis by the user.
- Academy loaned equipment:
    - Ensure that items of portable computer equipment, such as laptops, digital cameras or portable projectors are securely stored in a locked room or cupboard when left unattended.
    - Equipment taken offsite is not insured by the academy. If any academy computer equipment is taken offsite, it should be ensured that adequate insurance cover has been arranged to cover against loss, damage, or theft. Equipment must not be left in car boots.
    - Ensure personal or work software is not uploaded to academy's equipment without the permission of the Headteacher

- In order to keep accurate asset records, staff laptops must be checked and signed for on an annual basis. Failure to comply will result in re-appropriation of equipment.
- Laptops must be brought to academy every day and when not being used for planning must be used to support student learning and progression.

CONDUCT

- Staff must at all times conduct computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
  - Using, transmitting, or seeking inappropriate, offensive, gambling related, profit making, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials.
  - Making ethnic, sexual-preference, or gender-related slurs or jokes.
- Staff must ensure all Internet activity is appropriate to staff professional activity, including research for professional purposes. Where the system is made available for personal use, the same principles apply
- Staff must respect and not attempt to bypass, security or access restrictions in place on the computer system.
- Staff must not intentionally damage, disable, or otherwise harm the operation of computers.
- Staff must make efforts not to intentionally waste resources. Examples of resource wastage include:
  - Excessive storage of unnecessary files on the network storage areas.
  - Use of printers to produce class sets of materials, instead of using photocopiers.
- Staff should avoid eating or drinking around computer equipment.
- Staff must not use any academy facilities/resources in ways stated within the unacceptable use policy, which can found at the end of this document.

Social Media Policy

This policy is intended to provide the guidance required for employees to understand how to effectively and professionally use social media at work, and to understand the risk that is associated with this work. This policy also briefly covers the use of social media in employees personal capacity and it is important that employees are aware of the potential consequences that come with the use of social media whilst working in a public environment.

The Enquire Learning Trust is easy to identify, and all of us are very passionate about what we do. At the Enquire Learning Trust, we believe in open communication and you are encouraged to tell the world about your work and share your passion. There must however be some guidelines in place to avoid any problems or misunderstanding and as such this policy provides helpful and practical advice for you when operation on the internet.

1. Introduction

1.1 Social media sites have become important marketing tools as they allow users to interact and raise their profile with a wide cross section of other users. Blogging is also an important part of digital communication, and is used by a diverse range of businesses as well as individuals.

1.2 This policy and the procedures in it apply to any content that employees (including Governors) publish on the internet (e.g. their contributions in blogs, message boards, social networking sites or content sharing sites), even if created, updated, modified or contributed to outside of working hours or when using personal IT systems. This extends to both content which published on personal websites, blogs or social networking sites, and content which is published on corporate academy social media accounts.

Responsibilities of Employees

2.1 Any employees wanting to create a work-related social media site must discuss this with their academy Principal and obtain permission.

2.2 This policy covers all types of social media sites, including (but not limited to):

- Social networking sites e.g. Facebook, Instagram, Twitter and LinkedIn
- Blogging and micro-blogging sites
- Video clips and podcasts e.g. YouTube
- Discussion forums

2.3 Employees are personally responsible for the content they publish on social media sites – both personal and academy based.

2.4 Employees should not accept pupils as 'friends', unless there is a pre-existing relationship with the pupil (i.e. niece/nephew), and information must not be posted on personal social media accounts that would disclose the identity of pupils.

2.5 Pupils must not be named or discussed on personal social media sites.

2.6 Photographs or videos of pupils can only be posted if the consent form has been received and only posted on academy specific sites. They should never appear on personal social media sites.

2.7 Employees must not post information, including photographs and videos, on social media sites that could bring the academy or the Trust in to disrepute.

Corporate Responsibility

2.8 Employees must not represent their own views/opinions as being those of the academy or Trust. If you express any idea or opinion then you should add a disclaimer such as "these are my own personal views and not those of the academy".

2.9 Potentially defamatory remarks towards the academy, the Trust, employees, governors, pupils, pupils relatives, partner organisations must not be posted on social media sites.

2.10 Employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive or discriminatory language on social media sites.

2.11 Employees must not divulge any information that is confidential to the academy, Trust or a partner organisation.

2.12 The Trust expects employees at all times to conduct themselves appropriately when posting content on personal social media accounts, blog or website and in a manner which is consistent with your contract of employment and with academy policies and procedures.

2.13 It should be noted that individuals can be identified as working for the Trust simply by revealing their name or a visual image of themselves.

2.14 Employees who already have a personal blog or website that identified them as working for the Trust, or if employees have the intention to set up such a site, should notify their line manager.

2.15 The academy/Trust's logo or intellectual property may not be used in connection with any logging or social networking activity without permission from the Principal.

2.16 If employees think that something on a blog or website could give rise to a conflict of interest and in particular concerns issues or impartiality or confidentiality then this must be notified to the Principal.

2.17 No posts on any site should cause others embarrassment or harm in any way.

2.18 Employees should be mindful when placing information on social media sites that it is potentially visible to a large audience and could identify where they work and whom with thereby increasing the opportunity for false allegations and threats.

2.19 Employees must use appropriate security and privacy settings on social media sites in order to mitigate any potential issues, but should be aware that having restricted settings or profiles does not eliminate this risk entirely.

2.20 Employees should never provide references for other individuals on social or professional networking sites, as such references can be attributed to the Trust and create legal liability for both themselves and for the Trust.

Compliance with related policies and agreements

3.1 Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- Breach our e-safety and information governance policies and obligations with respect to the rules of relevant regulatory bodies
- Breach any obligations they may have relating to confidentiality
- Breach our disciplinary policies and procedures
- Defame or disparage the academy/Trust or its partners/stakeholders
- Harass or bully other employees in any way or breach or dignity at work policy
- Unlawfully discriminate against other employees or third parties or breach our equalities policy
- Breach our data protection policy
- Breach any other laws or ethical standards.

Monitoring

4.1 The contents of the Trust IT resources and communications systems are the Trust's property. Employees should have no expectation of privacy related to any type of communication made on Trust owned property, including personal communications.

4.2 Employees should be aware that all electronic communications are monitoring, including:

- Any message or email
- Files
- Data
- Internet usage
- Documents
- Telephone conversations
- Social media postings.

4.3 We may store copies of such data or communications for a period of time after they are created, and may delete such copies in line with data protection guidelines.

4.4 Do not use our resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

4.5 Be aware that any personal social media accounts have the potential to be accessed by stakeholders, including relatives of pupils, and ensure therefore that nothing is posted that may cause retaliation, upset, embarrassment or other unintended consequences for the organisation.

Any breach of this policy is likely to result in disciplinary action. A serious breach of this policy may be considered to amount to gross misconduct and therefore warrant summary dismissal.

This policy does not form part of any employees contract of employment and may therefore be amended at any time.

USE OF EMAIL

All members of staff with a computer account are provided with an email address for communication, both internally and with other email users outside the academy.

E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. Staff must be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail. Staff should regularly check email and delete older mail when it is no longer required.

SUPERVISION OF STUDENT USE

- Students must be supervised at all times when using academy computer equipment. When arranging use of computer facilities for students, staff must ensure supervision is available.
- Supervising staff are responsible for ensuring that the Student ICT Policy is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by students.

Enquire Learning Trust eSafety Policy

Principles and purpose

New technologies have become integral to the lives of children and young people in today's society, both within and outside their school lives. The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and Young people should have an entitlement to safe internet access at all times.

The use of these new technologies can put young people at risk, some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, sharing of personal information
- Risk of being subject to grooming by those with whom they make contact
- The sharing and distribution of personal images without their consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy and relevance of e-information
- Plagiarism and copyright infringement
- Illegal downloading of music and video files
- Excessive use impacting on social and emotional development

Scope of the Policy

This policy applies to all employees and students wherever they may be, both at school or elsewhere such as at home when accessing systems which the school is responsible for.

Roles and Responsibilities

Pupils

It is the responsibility of the students to:

- Keep themselves safe when using ICT
- Report any instances of intentional or non-intentional breaches to this policy

Staff

It is the responsibility of all who work with children within school to:

- Comply with this policy
- Ensure that they understand the risks that the students face
- Promote e-safety at every opportunity with students
- In the event of a disclosure report it to the appropriate Senior Leadership Team in school

E-Safety Coordinator

It is the responsibility of the e-safety coordinator to:

- Develop an eSafety culture
- Act as a named point of contact on all eSafety issues for the Senior Leadership Teams
- Promote the eSafety vision to all stakeholders and supporting them in their understanding of the issues
- Ensure that eSafety is embedded within the continuing professional developments for staff and co-ordinate training as appropriate
- Ensure that eSafety is embedded across the curriculum and activities within the organisation as appropriate
- Ensure that eSafety is promoted to all stakeholders
- Support pastoral teams to decide on appropriate sanctions for pupils
- Monitor and report on eSafety issues to the management team, other agencies and the local authorities eSafety lead as appropriate
- Develop an understanding of the relevant legislation
- Liaise with the local authority and other local bodies as appropriate
- Review and update eSafety policies and procedures on a regular basis

Principal/Head of School

The Principal/Head of School is responsible for:

- Ensuring appropriate arrangements are in place to comply with this policy
- Making sure all users are aware of this policy
- Ensuring that appropriate training is undertaken
- Ensuring that the technical infrastructure / network is as safe and secure as possible
- Updating the list of inappropriate websites which fall through the filtering software
- Supporting the investigation of eSafety incidents
- Applying sanctions to user accounts when necessary

Curriculum

1. All children will be given opportunities to:

    - develop word processing, spreadsheet, presentation and publication skills
    - develop control of wide range of hardware including tablets, laptops and computers.
    - develop an understanding on what ICT peripherals can be used to reach an end goal
    - use a range of multimedia software across the curriculum
    - use ICT to communicate with others
    - simulate and model situations
    - store, retrieve and communicate data effectively
    - use ICT to create music, video and animation
    - research and find out information
    - develop coding and programming skills
    - learn how to be safe online and how to prevent and deal with cyber-bullying
    - learn how to ensure that they work safely on ICT equipment e.g. posture and length of time using a device.
    - incorporate appropriate terminology in their work as well as make good use of ICT learning across the curriculum.
    - manage their own folder directories and file management
    - understand how networks and the world-wide web work
    - develop website building, blogging, wiki and other online skills

2. ICT is integrated across the curriculum, to support outstanding teaching, learning and assessment.

3. All staff and children have access to filtered Internet and the use of e-mail as a key communication tool

4. Children are given opportunities to use a range of technology including tablets, laptops, computers, Interactive whiteboards and screens, externally programmable devices, cameras, camcorders, audio records, headphones, printing and others peripherals

5. Staff will use ICT to inform and enhance their own professional practise.

6. The use of resources, hardware, and software will be managed, and increasing provision and future development will be planned accordingly.

7. All parents/guardians are required to sign a consent form for ELT and academies to use images of their child(ren).

8. All students are required to complete an Acceptable Use of ICT form. A list of children without consent is kept in each classroom and centrally by the admin team.

Enquire Learning Trust E-Safety Policy.

Staff Computer Security and Protection

Each member of staff will be provided with personal user account for accessing the computer system, with their own unique username and password. This account will be tailored with permissions to the level of access required and will be for that user's use only. Users must not disclose password information to anyone, including the ICT Technicians, or let other users use the computer systems under their logged on user account. In the event of a password becoming compromised, users will be required to change their password immediately by contacting the ICT Technicians.

- Passwords will be updated as per protocols decided by the Trust's Information Governance Policy.
- Personal computers and devices should not be used for work related purposes.
- Members of staff must not allow a student to have use of a staff account under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, it must be ensured that the computer is either logged off, or locked to prevent anyone using another's account
- USB memory sticks must not be used.
- When publishing, or transmitting non-sensitive material outside of the academy, staff must ensure they follow the appropriate guidance within the Information Guidance Policy
- Academy loaned equipment:
    - Ensure that items of portable computer equipment are stored securely
    - Equipment taken offsite is not insured by the academy. If any academy owned ICT equipment is taken offsite, it should be ensured that adequate insurance cover has been arranged to cover against loss, damage, or theft.
    - Equipment must not be left in cars for any length of time.
    - Ensure additional software is not installed onto any loaned ICT device unless permitted by the Strategic ICT Officer or Principal
    - To keep accurate asset records, portable devices assigned to staff, such as laptops, must be checked and signed for on an annual basis. Failure to comply will result in access to that equipment being revoked.

- Laptops must be brought to academy every day to ensure that key updates to Anti Virus, Operating System, and school specific software are processed to keep each device up to date and secure.
- Staff must always ensure they are working within the boundaries of the Trust Information Governance Policy.
- All staff are required to sign an Acceptable Use of ICT form annually in order to use the Trust and Academy ICT and systems

Further guidance around the processes below can be asked of the Trust's eSafety Team that consists of Brett Webster (Strategic ICT Officer), Liz Thompson (Governance Officer) and Jaimie Holbrook (Safeguarding Lead)

Incident Management process in the event of an eSafety incident

Action to be taken when the breach is made by a member of staff:

	Person Responsible
Where there is concern that there has been a breach of the eSafety Policy the person who is made aware of this will report this to the designated lead for eSafety/safe guarding	Member of Staff aware of the incident
The eSafety Co-ordinator will conduct an initial fact finding investigation which will ascertain who was involved, what has occurred. If appropriate the user will be restricted from access to the network	Principal/Head of School
The eSafety Co-ordinator will classify the incident appropriately (high or low severity) and enter details of the incident onto the member of staff's file	Principal/Head of School
The Principal/Head of School/line manager will have been informed and should be given the results of the initial fact finding investigation	Principal/Head of School
If appropriate discussions will take place between the Trust eSafety team and local ICT Technicians to implement any necessary actions e.g. blocking a website	Principal/Head of School
The Principal/Head of School/line manager will discuss the concerns with the Local Authority Designated Officer (LADO) in order to discuss whether there is a need for a Strategy Meeting. During this discussion consideration will be given as to whether the police need to be involved. The Principal/Head of School/line manager will also discuss with Lauren Stones (ELT HR Officer) if the member of staff needs to be suspended or undertake different duties pending the completion of the enquiries.	Principal/Head of School
The Principal/Head of School/line manager will also discuss the incident with the eSafety lead in the Trust as consideration will need to be given to any further actions required.	Principal/Head of School/Line Manager
The strategy meeting process will be completed.	
The designated lead will complete the agencies incident log and send a copy to the Trust's eSafety team	Principal/Head of School

Action to be taken when the breach is made by a pupil:

	Person Responsible
Where there is concern that there has been a breach of the eSafety Policy the adult will make a decision whether to deal with it themselves by applying a sanction and logging it in the relevant systems or report it to the Senior Leadership Team.	Member of Staff aware of the incident
The Senior Leadership Team will conduct an initial fact finding investigation who will ascertain who was involved, what sites have been accessed etc	Senior Leadership Team with support from the Principal/Head of School and ICT support
The Senior Leadership Team will classify the incident appropriately (high or low severity) and enter details of the incident into the relevant system and make a decision about appropriate sanctions, with support from the Trust's eSafety Team if necessary. They will also inform the ICT Technician's to enable them to make changes to the computer system if reduced access is required	Senior Leadership Team with support from Principal/Head of School and ICT support
If necessary, the Principal/Head of School/Head of School will discuss the concerns with the manager of the local authority safeguarding team to establish if there are child protection concerns requiring a Section 47 Child Protection investigation. If this is required the local Safeguarding Team will conduct this investigation as required within the Child Protection Procedures	Principal/Head of School

Enquire Learning Trust Social Media Policy

This policy is intended to provide the guidance required for employees to understand how to effectively and professionally use social media at work, and to understand the risk that is associated with this work. This policy also briefly covers the use of social media in employees personal capacity and it is important that employees are aware of the potential consequences that come with the use of social media whilst working in a public environment.

The Enquire Learning Trust is easy to identify, and all of us are very passionate about what we do. At the Enquire Learning Trust, we believe in open communication and you are encouraged to tell the world about your work and share your passion. There must however be some guidelines in place to avoid any problems or misunderstanding and as such this policy provides helpful and practical advice for you when operation on the internet.

1. Introduction

1.1 Social media sites have become important marketing tools as they allow users to interact and raise their profile with a wide cross section of other users. Blogging is also an important part of digital communication, and is used by a diverse range of businesses as well as individuals.

1.2 This policy and the procedures in it apply to any content that employees (including Governors) publish on the internet (e.g. their contributions in blogs, message boards, social networking sites or content sharing sites), even if created, updated, modified or contributed to outside of working hours or when using personal IT systems. This extends to both content which published on personal websites, blogs or social networking sites, and content which is published on corporate academy social media accounts.

2. Responsibilities of Employees

2.1 Any employees wanting to create a work-related social media site must discuss this with their academy Principal and obtain permission.

2.2 This policy covers all types of social media sites, including (but not limited to):

- Social networking sites e.g. Facebook, Instagram, Twitter and LinkedIn
- Blogging and micro-blogging sites
- Video clips and podcasts e.g. YouTube
- Discussion forums

2.3 Employees are personally responsible for the content they publish on social media sites – both personal and academy based.

2.4 Employees should not accept pupils as ‘friends’, unless there is a pre-existing relationship with the pupil (i.e. niece/nephew), and information must not be posted on personal social media accounts that would disclose the identity of pupils.

2.5 Pupils must not be named or discussed on personal social media sites.

2.6 Photographs or videos of pupils can only be posted if the consent form has been received and only posted on academy specific sites. They should never appear on personal social media sites.

2.7 Employees must not post information, including photographs and videos, on social media sites that could bring the academy or the Trust in to disrepute.

Corporate Responsibility

2.8 Employees must not represent their own views/opinions as being those of the academy or Trust. If you express any idea or opinion then you should add a disclaimer such as “these are my own personal views and not those of the academy”.

2.9 Potentially defamatory remarks towards the academy, the Trust, employees, governors, pupils, pupils relatives, partner organisations must not be posted on social media sites.

2.10 Employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive or discriminatory language on social media sites.

2.11 Employees must not divulge any information that is confidential to the academy, Trust or a partner organisation.

2.12 The Trust expects employees at all times to conduct themselves appropriately when posting content on personal social media accounts, blog or website and in a manner which is consistent with your contract of employment and with academy policies and procedures.

2.13 It should be noted that individuals can be identified as working for the Trust simply by revealing their name or a visual image of themselves.

2.14 Employees who already have a personal blog or website that identified them as working for the Trust, or if employees have the intention to set up such a site, should notify their line manager.

2.15 The academy/Trust’s logo or intellectual property may not be used in connection with any logging or social networking activity without permission from the Principal.

2.16 If employees think that something on a blog or website could give rise to a conflict of interest and in particular concerns issues or impartiality or confidentiality then this must be notified to the Principal.

2.17 No posts on any site should cause others embarrassment or harm in any way.

2.18 Employees should be mindful when placing information on social media sites that it is potentially visible to a large audience and could identify where they work and whom with thereby increasing the opportunity for false allegations and threats.

2.19 Employees must use appropriate security and privacy settings on social media sites in order to mitigate any potential issues, but should be aware that having restricted settings or profiles does not eliminate this risk entirely.

2.20 Employees should never provide references for other individuals on social or professional networking sites, as such references can be attributed to the Trust and create legal liability for both themselves and for the Trust.

Compliance with related policies and agreements

3.1 Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- Breach our e-safety and information governance policies and obligations with respect to the rules of relevant regulatory bodies
- Breach any obligations they may have relating to confidentiality
- Breach our disciplinary policies and procedures
- Defame or disparage the academy/Trust or its partners/stakeholders
- Harass or bully other employees in any way or breach or dignity at work policy
- Unlawfully discriminate against other employees or third parties or breach our equalities policy
- Breach our data protection policy
- Breach any other laws or ethical standards.

Monitoring

4.1 The contents of the Trust IT resources and communications systems are the Trust's property. Employees should have no expectation of privacy related to any type of communication made on Trust owned property, including personal communications.

4.2 Employees should be aware that all electronic communications are monitoring, including:

- Any message or email
- Files
- Data
- Internet usage
- Documents
- Telephone conversations
- Social media postings.

4.3 We may store copies of such data or communications for a period of time after they are created, and may delete such copies in line with data protection guidelines.

4.4 Do not use our resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

4.5 Be aware that any personal social media accounts have the potential to be accessed by stakeholders, including relatives of pupils, and ensure therefore that nothing is posted that may cause retaliation, upset, embarrassment or other unintended consequences for the organisation.

Any breach of this policy is likely to result in disciplinary action. A serious breach of this policy may be considered to amount to gross misconduct and therefore warrant summary dismissal.

This policy does not form part of any employees contract of employment and may therefore be amended at any time.

LINDEN ROAD ACADEMY AND CYBER BULLYING

Definition
Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend themselves.

Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.

Cyber-bullying, is bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones and devices
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, including but not limited to Facebook, Youtube, Snapchat and Ratemyteacher

At Linden Road we have zero tolerance of any form of bullying.

LEGAL ISSUES IN RELATION TO CYBERBULLYING

Cyber-bullying is generally criminal in character.
It is unlawful to disseminate defamatory information in any media including internet sites.
Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.
The wider search powers included in the Education Act 2011 give teachers stronger powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones.

Students are kept up to date in both the proper use of technology and about the serious consequences of cyber-bullying through the integrated curriculum which includes PSHE and computing learning sessions alongside assemblies, the Whizz Kids, website and involvement in events such as Anti-bullying Week and Safer Internet day.
All staff are aware of the need to respond effectively to reports of cyber-bullying or in line with the academy's anti-bullying policy

At Linden Road we support victims of cyberbullying and, when necessary, will work with the Police to detect those involved in criminal acts.
If cyberbullying is evident, this must be reported as per the Anti-bullying Policy immediately to the Principal

GUIDANCE FOR STAFF

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile phones and devices :

- Ask the student to show you the mobile phone
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names

- Make a transcript of a spoken message, again record date, times and names
- Tell the student to save the message/image. Take a screen shot.
- If the nature of the data is explicit do not forward the material as this could be illegal sharing of explicit images.
- Reassure the student.
- If a safeguarding concern is raised that this must be raised immediately with the Child Protection Office as outlined in the Safeguarding and Child Protection Policy.
- Immediately inform the Principal or member of Senior Leadership Team who will instigate the anti-bullying policy.

Computers:

- Ask the student to get up on-screen the material in question.
- Ask the student to save the material or take a screen shot.
- Do not print off or electronically share any explicit content or images.
- Re-assure the student
- Immediately inform the Principal or member of Senior Leadership Team who will instigate the anti-bullying policy.

GUIDANCE FOR STUDENTS

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible.
- Do not answer abusive messages or emails but log and report them
- Do not delete anything (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying)
- Do not give out personal IT details
- Never reply to someone you do not know
- Stay in public areas in chat rooms

GUIDANCE FOR PARENTS

- It is vital that parents and the academy work together to ensure that all students are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. We inform parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying via the website and news alerts.
- Parents can help by making sure their child understands the school's policy and, above all, how seriously Linden Road Academy takes incidents of cyber-bullying
- Parents should also explain to their sons or daughters legal issues relating to cyberbullying
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (by saving an offensive text on their or their child's mobile phone, mobile device or computer) Avoid deleting information. Parents should contact the Principal as soon as possible.
- If the incident outside of the normal school day and calendar the academy reserves the right to take action against bullying perpetrated outside the school which spills over into the school.
- Further up to date advice on cyberbullying and e-safety can be found on the academy website.

ACADEMY STAFF AND CYBER BULLYING

All academy staff are in a position of trust, and there are expectations that they will act in a professional manner at all times.

- Ensure you understand your school's policies on the use of social media, Childnet.com 'Using Technology' guide has more information on what to be aware of.
- Do not leave a computer or any other device logged in when you are away from your desk.
- Enabling a PIN or passcode is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by students.
- Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. Advice can be found on the Safer internet advice and resources for parents and carers.
- It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The UK Safer Internet Centres Reputation minisite has more information on this.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Use your school email address for school business and personal email address for your private life; do not mix the two.
- You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current student or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.
- If they refuse, it should be an organisational decision what to do next – either the school or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police. Online harassment is a crime.
- The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

PRIVACY

- Use of the academy computer system, including email accounts and storage areas provided for staff use, may be subject to monitoring by the academy to ensure compliance with this ICT Policy and applicable laws. In particular, the academy does keep a complete record of all websites visited on the Internet by both students and staff; however, usernames and passwords used are NOT monitored or recorded.
- Staff will not store personal information sensitive or otherwise on the academy computer system that is unrelated to academy activities (such as personal passwords, photographs, or financial information).
- The academy may also use measures to audit use of computer systems for performance and diagnostic purposes.

CONFIDENTIALITY AND COPYRIGHT

- Work and ownership rights of people outside the academy, as well as other staff or students, should be respected.
- Staff members are also responsible for complying with copyright laws and licenses that may apply to software, files, graphics, documents, messages and any other material which may be used, downloaded or copied.
- An ICT Technician must be consulted before the placing of any order relating to computer hardware or software or before obtaining and using any software believed to be free. This is to check that the intended use by the academy is permitted under copyright law, as well as to check compatibility and discuss any other implications that the purchase may have. The claims of suppliers should not be trusted, as they do not have specific knowledge of the academy computer system.
- Students are be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

REPORTING PROBLEMS WITH THE COMPUTER SYSTEM

It is the job of the ICT technician to ensure that the academy computer system is working optimally at all times and that any faults are rectified as soon as possible. In order to sustain this:

- Staff should report any problems that need attention to an ICT Technician as soon as possible by filling in ICT job sheets – located in ICT suite. Sheets to be left in ICT suite under whiteboard.
- If a computer has been affected by a virus or other malware or even suspected to have been, staff should report this to an ICT Technician immediately.
- Lost documents or files should be reported as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of data recovery.

ELT Acceptable Use Policy

The computer system is owned by the Trust and its academies. It is the responsibility of all who have access to the school system to abide by the computer usage policy. In practice this means that:

All Staff will:

- ☐ Ensure they understand and comply with the Information Governance and associated policies
- ☐ Only use the computer system for activities which relate the professional activity of students education or for acceptable personal usage outside teaching commitments
- ☐ Know that they have a responsibility for supervising pupils' usage of computer equipment
- ☐ Not use the computers for personal: financial gain, gamble, political purposes or advertising
- ☐ Respect copyright i.e. don't copy from the internet or from someone else without their permission
- ☐ Access pupils' files but only do so if it is relevant to their day-to-day work at school.
- ☐ Only access computer systems which they have been authorised to access, in an appropriate manner and for the agreed purpose
- ☐ Let no one else use their log in ID and passwords
- ☐ Keep their passwords secret and get them changed if they are found out
- ☐ Do not undertake any activity which threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems
- ☐ Not download and install software from the Internet or install programmes from USB drives, CD\DVD ROM, Floppy disk or other media onto any school computers (including laptops) – liaise with your ICT support provider for such installations
- ☐ Do not use any home or non-Trust devices for accessing information stored on the Trust network
- ☐ Lock computers if logged in when leaving the computer for any short period of time (a maximum of 10 minutes is advised)
- ☐ Log out when leaving the computer for an extended period of time (more than 30 minutes is advised or during break, lunch or lesson changeovers).
- ☐ Only use the network to access appropriate materials. Use of the network to access inappropriate materials such as pornography, or that contains reference to hate speech, racism, hacking, chat, violence, illegal music files, games or any sites that are not work related is forbidden.
- ☐ Not connect any personal equipment to the network
- ☐ Take care when sending emails, remembering that emails have the same legal authority as signed letters on official headed paper and therefore should treat them as such. They should not make personal comments in emails that could be used against the school and that they are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- ☐ Take care when receiving emails and do not open any suspect emails or attachments particularly where the sender is unknown, instead delete them. Notify someone in the event of receiving any threatening, lewd or inappropriate email
- ☐ Understand if they use their email for personal reasons (within the personal use guidance) that there is not a right of privacy
- ☐ Understand that the school views any misuse of its computer systems very seriously and that mis-use can include the following:
  - an attempt to access or actually access and/or use of any school computer system without authorisation
    - Revealing any information (by whatever means) from any computer system(s) to any unauthorised person or organisation

- Using the system or the information held within the system:
    - for other than its intended purpose,
    - other than in the authorised manner, or
    - for personal gain
- Failure to exercise due care in the use of school computer equipment and systems
- Copying any school software onto a non-school computer or device
- Using USB memory sticks
- Using the computer system for illegal usage such as national security, pornography, racism, hacking, fraud, communicating personal data, distributing copyrighted works e.g. music
- Using equipment, Internet or the e-mail system which is prejudicial to the school's interests or is defamatory or abusive
- Using the computer system for playing games
- Using email to distribute games or links to games
- Using proxy sites to circumvent the firewall

☐ Understand that the school has authority in reporting on all aspects of information, computer systems, Internet and e-mail usage and the recording of usage of computer systems, e-mail and the Internet, without the consent of the users

☐ Understand that non compliance may result in appropriate disciplinary, contractual and/or criminal action being taken within the context and spirit of the policy

Staff Agreement

I have read and understood ICT Policy for Linden Road Academy.

I understand that should I be found in breach of Policy I may be liable to disciplinary procedures and, if appropriate, the Police and local authorities may become involved.

I accept that it is my responsibility to be aware of amendments to this Policy which can be found on the staff server under the Staff Common drive.

Staff Name * _____ * USE BLOCK CAPITALS

Staff Signature _____ Date _____