IT and online safety policy

June 2017

Policy Statement

The Focus-Trust is committed to the creation and continual maintenance of a safe ICT and learning environment.

This policy identifies the essential elements of our Trust wide approach towards current and emerging technologies within all our academies and more importantly how our children and staffs' relationship operates with those technologies. Educating our children and staff to have safe behaviors whist being able to maximize the learning opportunities these technologies offer is key for all to thrive in the digital world.

We expect staff, pupils, visitors, contractors, and other employers to share this commitment by complying with our policies and procedures and to understand that they also have a legal and moral obligation to themselves and to others.

We believe that good technology management is an important and integral part of all employee's responsibility. The avoidance of significant risk to the safety of our children when they are online is a priority.

To do this effectively we will take a systematic approach to identifying risks and ensuring that resources are allocated proportionally to manage them. We require each academy to examine their own technology activities and make suitable and sufficient assessments of any risks. These assessments will determine academy priorities and set objectives for eliminating hazards, reducing risks and achieving a progressive and safe approach to technology management, usage and control.

The Trust Board recognizes the importance that strong leadership and effective management controls play a pivotal role in creating positive educational cultures towards the usage and approaches towards technologies.

On line safety places a responsibility on all staff to take reasonable care of their own safety and the safety of others. Teaching staff have a responsibility in loco parentis for the safety of all children within the school

The Trust Board accepts that it has a responsibility to ensure that effective and coherent procedures exists across the Trust and that they are continually monitored for their effectiveness.

It is the aim of the Trust Board and local governing bodies, 'To provide a safe working and learning environment for staff, pupils and visitors'.

The arrangements outlined in this Policy and the various other technology procedures cannot prevent accidents occurring but do aim to foster a "no blame culture" so that children and staff are able to report anything of concern to senior staff. However, the senior leaders within each academy will take all reasonable steps to identify and reduce hazards within its control to a minimum. All staff and pupils must appreciate

that their own safety depends on their individual conduct and vigilance whilst on line or on academy premises or whilst taking part in academy-sponsored activities.

Organisation
Overall accountability for technology usage lies with the Board, however, the day-to-day running of school technologies is delegated to the Principal and school management team. They have a responsibility in making sure all risks are managed effectively on site.
Sensible and effective management of IT technologies and systems relies on every member of the school management team making sure risk is managed responsibly and proportionately.

Focus Trust Board
As the employer, the Trust is responsible for making sure that risks, particularly the risks to staff and pupils, are managed so far as is reasonably practicable. IT functions are delegated to members of staff within the school to fulfil on behalf of the employer.

As the employer the Trust will…
- Put in place sensible approaches to IT technologies, with clear policies that focus on the real risks.
- Implement arrangements that manage the risks to staff, pupils and visitors who may be affected by school activities.
- Tell employees about the real and significant risks in the school and the precautions they need to take to manage them
- Make sure employees have the relevant information and training to manage risks on a day to day basis, including access to competent IT advice.
- Check that control measures have been implemented and remain appropriate and effective .

The Governors
- Take reasonable steps to make sure that the school is following the employer's policy and procedures e.g. through regular discussion at governance meetings.
- Ensure staff receive adequate training to enable them to carry out their responsibilities.
- Promote a sensible approach to on line safety, making use of competent IT advice when required.
- Work in close partnership with the Principal and senior management team to support sensible IT management and to challenge as appropriate.

Principal
Principals and the school management team/ manager have considerable autonomy in the day-to-day running of their schools. It is important that they exercise this autonomy in line with the Trusts policies, procedures and standards.

The Principal must;
- Ensure that the school is following the Trusts IT and on line safety policy and has effective arrangements for managing the real on line risks at the school.
- Maintain effective communications with employers, governors, and the school workforce, and give clear information to pupils and visitors, including contractors, regarding the IT risks.

- Make sure that staff have the appropriate training and competencies to deal with risks in their areas of responsibility.
- Make sure that staff understand their responsibilities and know how to access support and advice to help them manage risks responsibly.

Other School Leaders
The IC Lead, business manager and or, the IT contractor often take on the lead for IT technologies on site. They often provide the focal point for the school's IT management arrangements. Their school wide roles may include:

- management and monitoring of purchasing IT technologies
- advising contractors of current IT issues and overseeing their activities on site
- ensuring staff and visitors are aware of IT procedures and the precautions to follow
  reporting on anything of concern
- implementation, monitoring and review of training procedures
- preparation of reports and returns for the school leadership team

Action by each school – As the requirements and skill sets are different in each school specific roles and responsibilities must be identified at school level and documented in the 'front section" of each school policy.

Teachers
Have expertise in their topic areas and are in the best position to advise or lead on the arrangements for assessing and managing risk in their classrooms

- Schools may appoint a IT teaching specialist or another nominated lead to take a primary role in providing support across the school's range of on line learning activities.

Nominated IT leads should:

- have sufficient authority to take the lead responsibility for IT
- have time, resource and competence to fulfil the role

Staff
The school workforce play an important part in using IT technologies appropriately. All staff need to ensure that they process the skills and knowledge to teach children and parents about keeping safe on line. An educational approach to technologies is vital to enable children and adults to thrive in the digital world. Being a critical thinker is the greatest asset a teacher can imparts on to a child to enable them to maximize their usage of technologies.

Staff must

- Take reasonable care for your on line safety and that of others who may be affected by their actions.
- Be familiar with the schools IT and online policy
- Ensure IT, rules, routines and procedures are being applied effectively by both staff and pupils.
- Cooperate with the Principal and Focus Trust Board, fellow members of staff, contractors and others to enable them to make and keep safe.
- Raise IT and online safety concerns in line with local arrangements.
- Be familiar with e-bullying/cyber bullying and bring concerns to those who need to act on it

- Know how to respond to incidents of concern e.g. "sexting, indecent images, in-appropriate searches, "Prevent" related issues

Hirers, contractors and others

- When the premises are used for purposes not under the direction of the Principal/Head of Academy, then the person in charge of the activities for which the premises are in use will ensure that they make no attempt to use the schools IT systems.

- The Principal/Head of Academy, via the Business Manager and the Site Supervisor, will seek to ensure that hirers, contractors and others are unable to access school IT systems. These means that all systems are either locked away or have strong password protection.

Staff consultative arrangements

- The Principal/Head of Academy will incorporate agenda items on IT matters into meetings of existing consultative groups. Management, standing committees and consultation meetings with professional association representatives will consider IT safety matters as appropriate.

Arrangements

Codes of practice and safety rules

- The implementation of this Policy is supported by the Focus-Trust IT and online Safety Manual (A-Z). This contains arrangements, protocols and procedures for implementation at academy level.

- From time to time the Department for Education (DFE), the IOC and other regulatory or advisory bodies will issue codes of practice on particular topics for the guidance of Heads and others who are in control of educational premises, who will normally incorporate such codes into their site specific IT and Online safety procedures.

- All policies and handbooks are available to all staff members.

Risk assessment

- The Senior Management Team will ensure that risk assessment of IT technology systems are undertaken and compliance with statutory obligations within individual schools, audits and inspections are carried out from time to time.

Review

- The Trust Board will review this policy statement from time to time and update, modify or amend it as it considers necessary to ensure the health, safety and welfare of staff and students. This review will be a minimum of every two years and after any serious accident.

Title	IT and On line safety Policy
Aim	To provide a consistent policy position on ICT technologies
Related documents	IT safety Manual
Date for implementation	Immediately
Approved by	Trust Board –
Date of next review	Annually
Reviewed	Reviewed

Note -
Within the context of this document:

- 'Business manager' should be read to include 'Senior Business Manager'
- 'Principal' and 'Head' should be read to include 'Executive Principal', 'Principal' and 'Head of Academy'.

ICT Technologies safety manual (A-Z) - Index

This manual provides documents to help implement the requirements of the Trusts IT and On Line Safety Policy.

The ICT technologies manual is reviewed annually and academies will be notified of any updates.

Document Name	Last Updated
Academy networks, equipment and data safety	June 2017
Complaints, allegations and infringements	June 2017
Digital video, images, web site, learning platforms and CCTV systems	June 2017
Education and training	June 2017
Email usage and safety	June 2017
Email usage and safety – compliance forms	
Safety Protocols	June 2017
Social media	June 2017

Title **Academy networks, equipment and data safety**
June 2017

The purpose of this Section is to give academies an understanding of the principles, which should be followed in the setting up networks, purchasing and managing equipment and data safety.

All new employees must be shown all the IT procedures on their first day. Schools must ensure that all staff are aware of data protection protocols, on line safety training, equipment storage and network monitoring procedures as soon as practicable.

Academy networks

Technical and Infrastructure approaches

All Academies within the Trust will:

- Have filtered secure broadband connectivity;
- Use a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc;
- Ensure network health through use of anti-virus software so staff and pupils cannot download executable files;
- Use individual, audited log-ins for all users;
- Use DfE approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Block all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblock other external social networking sites for specific purposes i.e Internet Literacy lessons;
- Only use an approved service for video conferencing activity;
- Only use approved or checked webcam sites;
- Block pupil access to music download or shopping sites – except those approved for educational purposes such as Audio Network;
- Use security time-outs on Internet access where practicable/useful;
- Provide highly restrITed (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils;
- Provide staff with an email account for their professional use and make clear personal email should be through a separate account.
- Use a managed/monitored system that provides reports and alert senior managers if the systems is being inappropriately used.

Using the academy network, equipment and data safety

Using the academy network, equipment and data safely

The computer system / network is owned by the Focus-Trust and is made available to staff and pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely academies within the Trust:

- Ensure staff read and sign that they have understood the school's on-line safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform *and (for older pupils) their own school approved email account*;
- Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrITions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have 'crashed'. (We request that they DO switch the computers off at the end of the day);
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed, e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved suppliers/electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is restrITed and access is only through school approved systems:

- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restrITed and is only through approved systems;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- All our wireless networks must be secured to industry standards appropriate for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high.

Title Complaints, allegations and infringements
June 2017

The purpose of this Section is to give academies an understanding of the principles of how staff and children deal with complaints, allegations and infringements.

Complaints

The Trust will take all reasonable precautions to ensure Online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the academy nor the Trust can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Any complaint should be referred to the academy Principal – see Complaint Policy.

Allegations

It is essential that any allegation made against a teacher or other member of staff or volunteer is dealt with fairly, quickly, and consistently (See Focus-Trust and Academy Safeguarding Policies for more details)

Cyber bullying

Complaints about so-called cyber-bullying are dealt with in accordance with our Anti-Bullying Policy and, where necessary, Safeguarding Procedures.

Everyone should minimise the potential for and be aware of the impact of cyberbullying, which might include:

- Sending threatening or disturbing text messages;
- Homophobia, racism or sexism;
- Making silent, hoax or abusive calls;
- Creating and sharing embarrassing images or videos;
- 'Trolling', the sending of menacing or upsetting messages on social networks, chat rooms or online games;
- Excluding children from online games, activities or friendship groups;
- Setting up hate sites or groups about a particular child;
- Encouraging young people to self-harm;
- Voting for someone in an abusive poll;
- Hijacking or stealing online identities to embarrass a young person or cause trouble using their name;
- Sexting - which may be done to pressure a child into sending images or engaging in other unsafe and / or inappropriate activity.

We adopt a zero-tolerance approach to all forms of bullying behaviour and expect pupils and parents to do the same. **Any** concerns about online or cyberbullying should be reported to the Academy's Designated Safeguarding Lead without delay.

Infringements

Whenever a student or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the academy and Trust management and will reflect the Trust's disciplinary procedures.

The following are for example only:

STUDENT	
Category A infringements	**Possible Sanctions:**
- Use of non-educational sites during lessons - Unauthorised use of email - Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends - Use of unauthorised instant messaging / social networking sites	Refer to class teacher Escalate to: senior manager / Online safety Coordinator
Category B infringements	**Possible Sanctions:**
- Continued use of non-educational sites during lessons after being warned - Continued unauthorised use of email after being warned - Continued unauthorised use of mobile phone (or other new technologies) after being warned - Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups - Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc - Trying to buy items over online - Accidentally corrupting or destroying others' data without notifying a member of staff of it - Accidentally accessing offensive material and not logging off or notifying a member of staff of it	Refer to Class teacher or senior leader Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent
Category C infringements	**Possible Sanctions:**
- Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. - Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) - Trying to access offensive or pornographic material (one-off) - Purchasing or ordering of items online - Transmission of commercial or advertising material	Refer to Principal Escalate to: contact with parents / removal of equipment Other safeguarding actions if inappropriate web material is accessed: Ensure appropriate technical support filters the site
Category D infringements	**Possible Sanctions:**
- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned - Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent - Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 - Bringing the academy or Trust name into disrepute	Refer to Principal / Contact with parents (unless to do so might place a child at risk, impede an investigation or cause undue delay leading to either of the above) Other possible safeguarding actions: - Secure and preserve any evidence - Inform the sender's e-mail service provider. - Liaise with relevant service providers/ instigators of the offending material to remove - Report to Police / CEOP where child abuse or illegal activity is suspected
STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. - Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. - Not implementing appropriate safeguarding procedures. - Any behaviour on the World Wide Web that compromises the staff member's professional standing in the school and community. - Misuse of first level data security, e.g. wrongful use of passwords. - Breaching copyright or license e.g. installing unlicensed software on network.	Referred to Principal Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software; - Any deliberate attempt to breach data protection or computer security rules; - Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; - Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; - Bringing the school name into disrepute	Referred to Head teacher, Governors. Other safeguarding actions: - Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. - Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. - Where it is suspected that behaviour or imagery is indecent or where it is suspected that a criminal offence may have been committed: *Escalate to:* *- Report to Personnel, Human Resources for action;* *- Refer to Children's Services and / or* report to Police / CEOP where child abuse or illegal activity is suspected.

Where an Allegation is made Against a Member of Staff

Keeping Children Safe in Education (Part four) defines an allegation as :

"... all cases in which it is alleged that a teacher or member of staff (including volunteers) in a school or college that provides education for children under 18 years of age has:

- **behaved in a way that has harmed a child, or may have harmed a child;**
- **possibly committed a criminal offence against or related to a child; or**
- **behaved towards a child or children in a way that indicates he or she would pose a risk of harm to children**.

The person to whom an allegation is made or who observes a worrying incident, conduct or behaviour from an adult in school should report this immediately to the Principal (or the Chair of the LGB if the concern is about the Principal. The Principal / Chair of Governors then becomes the 'case manager' and should establish the basic facts which underpin the concern / allegation. **Note:** They should do so without investigating, i.e. trawling, interviewing staff or children, and decide whether there is the possibility that the matter meets the allegations threshold - above.

The Principal / case manager, will consult with the LADO and any notifications and onward referrals made to Police and Children's Services where appropriate. Focus Trust and LSCB safeguarding / managing allegations procedures will be adhered to.

Matters relating to suspension, the provision of support for the subject of the allegation and any disciplinary proceedings will be implemented in-line with these procedures and Part Four of Keeping Children Safe in Education 2016.

In the case of inappropriate or abusive images being found or linked to a member of staff or other adult in school, any equipment accessed by the individual concerned may be secured but *only* where *this can be achieved without raising suspicion which may result in the contamination or loss of evidence* - and the procedure at 6.3. followed.

Such matters must always be reported immediately to and next steps agreed with Police. Under these circumstances, the member of staff must not be alerted to the allegation without the agreement of the investigative agencies, especially where a

crime has or may have been committed. The Head of HR and Chief Executive must also be notified as soon as possible.

Potentially Indecent Images not Linked to an Adult in School
If potentially indecent images of children are found in any other circumstance (for example on a pupil's phone) the Police will be called immediately and advice sought regarding next steps.

Any inappropriate or potentially illegal online activity or suspected abuse which does not relate to a professional can be reported to the Child Exploitation and Online Protection Centre(CEOP) which is part of the National Crime Agency:

http://www.ceop.gov.uk/reporting_abuse.html

Title **Digital video, images, web site, learning platforms and CCTV systems June 2017**

The purpose of this Section is to give academies an understanding of the principles, which should be followed in the managing digital videos, images and CCTV systems and data safety.

Use of digital video and images

Academies within the Trust:

- Gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the academy;
- Ensure relevant staff are made aware of any pupil whose parent has withheld consent
- Digital images /video of pupils are stored in a private teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- If digital images are stored on drop box or other "clouds" storage areas, access to those images need to have strong password protection
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their Online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse, including from peers.

Website

- The Principal takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers;
- The school website complies with the Trust's guidelines for publications;

- Most material is the school's own work - where other's work is published or linked we credit the source(s)used and state clearly the author's identity or status;
- The point of contact on the web site is the school address / telephone number - we use a general email contact address rather than for a specific person.
- Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers using school approved blogs or wikis to password protect them.

Learning platform

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the academy or Trust platform will only be accessible by members of the Trust community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform;
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' Learning Platform for such communications.

CCTV

- Where CCTV is used, we will not reveal any recordings (*retained by the Support Provider for 28 days*) without permission, except where disclosed to the Police as part of a criminal and / or child protection investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the Trust and will not use for any other purposes.

Title **Education and training**
June 2017

The purpose of this Section is to give academies an understanding of the principles of how staff and children should be educated in the usage, staying safe and ensuring that both staff and children are able to report when they are uncomfortable with what they are seeing, hearing on the range of technologies available to them.

Training

Pupils

- An Online safety training programme will be is used to raise the awareness and importance of safe and responsible internet use. Instruction in responsible and safe use should precede Internet access;
- An Online safety module will be included in the PSHE, Citizenship or IT programmes covering both school and home use;
- Older pupils should be made aware that internet traffic is monitored and can be traced to the individual user.

Staff

- Staff should be made aware that Internet use is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff should also be advised that any use of the internet for purposes which are illegal or which may bring the profession into disrepute (such as viewing online images of children, inciting racial hatred, etc) will lead to disciplinary and, where necessary, criminal action. This applies to conduct both in and outside the work environment.
- Staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting any concerns.
  According to Keeping Children Safe 2016, our systems and training must enable us to identify individual children who may be at risk. Our procedures should ensure that everyone knows what to do next to protect them.
- Staff training in safe and responsible Internet use and on the school Online safety Policy will be provided and updated annually.

Parents and carers

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be adopted. This could include parent workshops with demonstrations and suggestions for safer home IT use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents
- Making relevant and up-to-date resources available via Academy websites, newsletters and school events
- Appendix F will be shared with all new parents and annually as part of online safety updates and training

Education:

Academies within the Trust:

- Foster a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teach pupils and inform staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher, ICT leader, or Principal.
- Ensure pupils and staff know what to do if there is a cyber-bullying incident;
- Ensure all pupils know how to report any abuse;
- Have a clear, progressive Online safety education programme throughout all Key Stages, built on national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - Working with older children to help them understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand 'Netiquette' behaviour when using an online environment/ email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why Online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not take, post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- Ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also

know that they must observe and respect copyright / intellectual property rights;

- Ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying Online; Online gaming / gambling;
- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Make training available annually to staff on the Online safety education program;
- Run a rolling programme of advice, guidance and training for parents, including:
  - information leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions held at school;
  - distribution of 'think u know' for parents materials
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

The computing curriculum sets out in detail the technical skills and some of the legal knowledge that a child should have at different ages, there is a view that this is too little too late, and that the essential 'social' elements of life online are not consistently taught, e.g. how other people portray their lives online, how to spot fake news, how to disengage and control your use. What children need is a full enough range of skills so that they can navigate what is an undeniably social space.

Induction training for staff and governors

Training for new staff is an integral part of their induction and safeguarding training. Existing staff receive online updates about online safety matters as part of an annual Online Safety Week across the Trust.

As part of the whole school approach governors are trained and provided with updates to empower them to ask the right questions and ensure that what is in place is fit for purpose and effective.

Title **Email usage and safety – compliance forms**
June 2017

Form 1 Responsible internet use for pupils

Keeping safe: stop, think, before you click!

15 rules for responsible IT use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for schoolwork and homework.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will keep my logins and passwords secret.
4. I will not bring files into school without permission or upload inappropriate material to my workspace.
5. I am aware that some websites and social networks have age restrictions and I should respect this.
6. I will not attempt to visit Internet sites that I know to be banned by the school.
7. I will only e-mail people I know, or a responsible adult has approved.
8. The messages I send, or information I upload, will always be polite and sensible; including email and social messaging
9. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
10. I will not bring CDs, DVDs or USBs from outside school unless I have been given permission.
11. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
12. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
13. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
14. I understand that the school can check my computer usage and everything that I do can be seen; even if I delete it. I know that if I do not follow the rules I must accept the consequences and discipline.
15. I must ask permission to use the school printers and print only one copy of a document.

Name	
Academy name	
Signed (parent/carer)	
Signed (pupil)	
Date	

Form 2: Acceptable Use Policy for staff and volunteers

The computer system (including lap tops) is owned by the Focus-Trust and is made available to staff to enhance their professional activities, including teaching, research, administration and management. The Trust's Acceptable Use Policy has been drawn up to protect all parties – the pupils, the staff and the Focus-Trust.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- That the Trust's IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk; and
- That staff are protected from potential risk in their use of IT in their everyday work.

The Focus-Trust will try and ensure that staff and volunteers have good access to IT to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

The Focus-Trust reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff should be aware that files and/or hardware will be handed to the Police or law enforcement agency.

Acceptable Use Policy Agreement

I understand that I must use the Trust's systems and equipment in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, educate young people in my care in the safe use of IT and embed Online safety in my work with pupils.

For my professional and personal safety:

1. I understand that the Focus-Trust will monitor my use of the IT systems, email and other digital communications.

2. I understand that the rules set out in this agreement also apply to the use of Trust IT systems and equipment when used off-site.

3. I understand that the IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies set down by the Trust.

4. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

5. I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

6. I will be professional in my communications and actions when using the IT systems:
    a. I will not access, copy, remove or otherwise alter any other user's files, without their express permission. This includes files on the shared intranet.
    b. I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

c. I understand that email can be forwarded or inadvertently sent to the wrong person, the same levels of language should be applied as for the letters or other media.
d. I will ensure that when I take and/or publish images of others I do so with their permission and in accordance with the Trust's policy on the use of digital images/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.
e. I will only use chat and social networking sites in accordance with the Trust's policies.
f. I will only communicate with pupils and parents using the official systems. Any such communication will be professional in tone and manner.
g. I will not engage in any Online activity that may compromise my professional responsibilities.

7. The Academy and Trust have the responsibility to provide safe and secure access to technologies.
    a. When I use my personal devices (incl phone, hand held, lap top, USB, iwatches, etc), I will follow the rules set out in this agreement, in the same way as if I was using fixed equipment. I will also follow any additional rules set about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
    b. I will not use personal email addresses on the Trust IT system.
    c. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
    d. I will ensure that my data is regularly backed up.
    e. I will not try to upload, download or access any materials which are illegal (child sexual abuse, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
    f. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent others from being able to carry out their work.
    g. I will not install or attempt to install programmes of any type on a machine, or store programmes on a PC, not will I try to alter computer settings, unless this allowed in a specific policy.
    h. I will not disable or cause any damage to school equipment, or the equipment belonging to others.
    I understand that what is on my device is my responsibility and I am accountable.

8. I will only transport, hold, disclose or share personal information about myself or others as outlined in the Trust's Data Policy. Where personal data is transferred outside the Trust network, it must be encrypted.
    a. I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except where it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority.
    b. I will immediately report any damage or faults involving equipment or software, however this may have happened.

9. When using the internet in my professional capacity or for sanctioned personal use:
    a. I will ensure that I have permission to use the original work of others in my own work.

b. Where work is protected by copyright, I will not download or distribute copies (including music and videos).

10. I understand that I am responsible for my actions in and out or work:
    a. I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in work, but also applies to my use of Trust IT systems and equipment out of work and my use of personal equipment in school or in situations related to my employment by the Trust.
    b. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, suspension, dismissal. I understand that all illegal activities will be reported to the Police and relevant law enforcement agencies.

11. I will ensure that any use of social media does not:
    - bring the academy and/or the Trust into disrepute;
    - breach confidentiality;
    - breach copyrights of any kind;
    - bully, harass or be discriminatory in any way; and
    - cannot be classified as defamatory or derogatory.

Anyone who uses laptops and/or other property from the school will assume all liability and responsibility for safeguarding it while it is loaned out to them.

Please take the following precautions:

- If you take your laptop home, be sure to lock all doors when you go out. If you have a home security system, be sure it is on when you leave.
- Keep laptop in your sight when travelling on public transport.
- If you are travelling by car, lock your laptop in the boot when you park.
- Do not use the laptop in locations that might increase likelihood of damage.
- Keep food and drinks away from the laptop.

If the laptop is lost/stolen on the way from school, at home or on the way to/from school; or if it is damaged despite proof of you having followed the guidelines listed above, no further action will be taken. When equipment is lost, stolen, or damaged and the above guidelines were not followed the user will pay all replacement or repair costs at the current market value. The Trust may also take disciplinary action where it is considered that an act of negligence has led to damage or theft of school-owned equipment.

If you have homeowner's insurance, that policy may cover part, or all, of the costs. Teachers should notify their insurance company and have some coverage in that manner.

I have read and understand the above and agree to use the Trust IT systems (both in and out of work) and my own devices (in work when carrying out communications related to work) within these guidelines.

Name	
Academy name	
Signed	
Date	

Title **Email usage and safety**
June 2017

The purpose of this Section is to give academies an understanding of the principles, which should be followed in the managing email usage and safety with emails

Email usage and safety

The Trust

- We do not publish personal e-mail addresses of pupils or staff on the Trust or academy website.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the Police.
- Accounts are managed effectively, with up to date account details of users.
- Messages relating to or in support of illegal activities will be reported to the relevant authority and Police.
- We use an anti-virus product and additional email spam, phishing software.

Academy and central Trust staff

- Staff use Focus-Trust e-mail systems for professional and work purposes.
- Staff are only allowed to use the Focus-Trust domain e-mail accounts on the school systems (ipads, ect).
- We never use email to transfer pupil level data. We use secure, DFE approved systems. These include: S2S (for school to school transfer); secure XML transfer of management information data transfer; *USO-FX*.
- Staff are not permitted to use a personal email account for professional purposes.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the Trust 'house-style';
- The sending of multiple or large attachments should be limited;
- Personal information must not be sent as attachments on open email. A secure method of encrypted transfer should always be used.
- The sending of chain letters is not permitted.
- Embedding adverts is not allowed.
- Staff know that all emails may be monitored.
- Staff know that their account details and any Trust equipment will be handed to police or law enforcement organisations should the need arise;
- Staff know that all emails sent from their account are traceable, regardless of deleted emails.
- All staff sign the Trust acknowledgment form to say they have read and understood the Online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Pupils

- We use communication tools within the 'closed' Learning Platform with the pupils for communication with staff and other pupils. All this is audited.
- We do not use email that identifies the name and school of the pupil.
- Pupils are introduced to, and use e-mail as part of the IT scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and more generally (for example personal accounts set-up at home) i.e.

- not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- the sending of multiple or large attachments should be limited;
- personal information should not be sent as attachments on open email. A secure method of encrypted transfer should always be used;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

Action

Pupils sign the school Agreement Form to say they have read and understood the Online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

During the academic year academies will go some way towards ensuring then 'road-testing' the effectiveness of training and education around safer use of technologies. For example:

- Via the use of online safety surveys with pupils to see what they are using and, therefore, what skills they need;
- Via annual safeguarding audits which include conversations with mixed groups of pupils around the issues.

Academies will take into consideration the findings of the PSHE Association / CEOP 'How to Protect' report (April 2016) about the essentiality of education which:

- is part of a whole school approach involving multiple interventions, parents etc.
- Uses varied teaching styles and active, skills-based learning
- is appropriate to age and maturity
- Non confrontational / avoid scare tactics
- is of adequate length and intensity

Title **Safety Protocols**
June 2017

The purpose of this Section is to give academies an understanding of the principles of how staff and children should behaviour to maintain data safety in the digital world.

Digital security

Within the Trust:

- All staff, pupils and parents sign the Acceptable Use Agreement form. Copies are kept on file. This makes clear staffs responsibilities with regard to data security, passwords and access.
- All staff are DBS checked and records are held in one central record.
- Focus Trust require staff to use strong passwords for access into all MIS systems.
- Focus Trust require staff to change their passwords into the MIS at least twice a year.
- Staff have a secure area on the network to store sensitive documents or photographs.
- Focus Trust require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 mins idle time. (time outs in class rooms may differ due to a teacher delivering lessons)
- Staff know who to report any incidents where data protection may have been compromised.
- Focus Trust require that any Protect and Restricted material must be encrypted if the material is to be removed from the school. We encrypt flash drives for this purpose and limit such data removal.
- Focus Trust use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- Focus Trust store any Protect and Restricted material that is in an un-encrypted format (such as paper) in lockable storage cabinets in a lockable storage area.
- All servers are managed by CRB/DBS-checked staff.
- Focus Trust ask staff to undertake at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- Each school must use a recognised confidential disposal company for disposal of system hard drives where any protected or restricted data has been held.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder.

Protective Marking levels

The combined force of the Data Protection Act and Data Handling Procedures in Government make it critical to recognise the sensitive personal data held and to protect and secure personal data. To ensure a uniform method of assessing the impact of potential compromises to the confidentiality, integrity or availability of information and information systems, and provide comparable levels of information protection when the data is shared, the Government Protective Marking Scheme is used to indicate the sensitivity of data. This comprises five markings. In descending order of sensitivity they are:

- TOP SECRET
- SECRET

- CONFIDENTIAL
- RESTRICTED
- PROTECT

Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

Protective markings should be marked in the subject line of emails or at the top of documents.

Most Learner or staff personal data that is used within schools comes under the PROTECT classification.

Criteria for assessing PROTECT assets:

- cause distress to individuals;
- cause risk to the Trust;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- breach statutory restrictions on the disclosure of information
- cause financial loss or loss of earning potential, or to facilitate improper gain;
- unfair advantage for individuals or companies;
- prejudice the investigation or facilitate the commission of crime;
- disadvantage government in commercial or policy negotiations with others.

Criteria for assessing RESTRICTED assets:

- affect diplomatic relations adversely;
- cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness or security of United Kingdom or allied forces;
- cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies;
- prejudice the investigation or facilitate the commission of crime;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- impede the effective development or operation of government policies;
- to breach statutory restrictions on disclosure of information;
- disadvantage government in commercial or policy negotiations with others;
- undermine the proper management of the public sector and its operations.

Criteria for assessing CONFIDENTIAL assets:

- materially damage diplomatic relations (i.e. cause formal protest or other sanction);
- prejudice individual security or liberty;
- cause damage to the operational effectiveness or security of United Kingdom or allied forces or the effectiveness of valuable security or intelligence operations;
- work substantially against national finances or economic and commercial interests;
- substantially to undermine the financial viability of major organisations;
- impede the investigation or facilitate the commission of serious crime;
- impede seriously the development or operation of major government policies;
- shut down or otherwise substantially disrupt significant national operations.

What measures should schools take?

It is a legal requirement to protect sensitive data, and Data Handling Procedures in Government sets out the measures that schools should adopt to maintain data security:

- Users may not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely for storage in a secure location.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Sensitive or personal data must be securely deleted when it is no longer required.
- For schools, this means that they must encrypt any data that is classified as Protect (or higher) if this data is removed or accessed from outside any approved secure space such as a school or Trust offices. Education organisations must also ensure that data classified as Protect or higher is encrypted when it is in transit from one location to another, including transit from one approved secure location to another.

Summary of the **Dos and Don'ts**

Data Security

Passwords - Do

- use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)

Passwords - Don't

- ever share your passwords with anyone else or write your passwords down
- save passwords in web browsers if offered to do so

Laptops - Do

- try to prevent people from watching you enter passwords or view sensitive information
- log-off / lock your 'desktop' when leaving your PC or laptop unattended.

Sending and sharing - Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner(s) if you are not sure.
- only use encrypted removable media (such as encrypted USB pen drives) if ever taking any 'Protected' data outside your school.

Sending and sharing - Don't

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives), if secure remote access is available.
- send sensitive information by email unless it is encrypted; Pupil data must be sent via S2S (DFE secure web site)

Working on-site - Do

- lock sensitive information away when left unattended, i.e. in lockable drawers, log off or lock work station

Working on site - Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

Working off-site - Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above
- wherever possible access data remotely instead of taking it off-site - using approved secure authentication
- make sure you sign out completely from any services you have used
- ensure you save to the appropriate area to enable regular backups

Title	Social media
	June 2017

The purpose of this Section is to give academies an understanding of the principles, which should be followed in the managing of social media.

Social media

Introduction

- The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopedias such as *Wikipedia*.
- While recognising the benefits of these media for new opportunities for communication, this guidance sets out the principles that all Focus Trust staff and contractors are expected to follow when using social media.
- It is crucial that pupils, parents and the public at large have confidence in the Focus Trust's decisions and services. The principles set out in this guidance are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the academy and Focus Trust are safeguarded.

- Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Scope

- This guidance applies to All Focus Trust staff, all teaching and other staff, whether employed by the Focus-Trust, external contractors providing services on behalf of the academy or the Focus-Trust, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the academy or Focus Trust. These individuals are collectively referred to as 'staff members' in this guidance.

- This guidance covers personal use of social media as well as the use of social media for official academy purposes, including sites hosted and maintained on behalf of each academy. Only designated staff are allowed to post on school media sites.

  This guidance applies to personal webspace such as social networking sites (for example *Facebook*, *MySpace*), blogs, mircoblogs such as *Twitter*, chatrooms, Forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this guidance must be followed irrespective of the medium.

Legal Framework

- Focus Trust is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the academy or the Trust are bound by a legal duty of confidence and other laws to

protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- the Data Protection Act 1998.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- Academy or Focus-Trust business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

The Focus-Trust or one of the academies within the Trust could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render the academy or the Focus-Trust liable to the injured party.

Related Policies/guidance

This guidance should be read in conjunction with the following Focus-Trust policy:

- Staff Code of Conduct

Focus Trust Principles will always be; – be professional, responsible and respectful.

You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the academy or Focus-Trust and your personal interests.

You must not engage in activities involving social media which might bring the academy or the Focus-Trust into disrepute.

You must not represent your personal views as those of the academy or the Focus-Trust on any social medium.

You must not discuss personal information about pupils, The academy or Focus-Trust staff and other professionals you interact with as part of your job on social media.

You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, the academy or the Focus-Trust.

You must be accurate, fair and transparent when creating or altering online sources of information on behalf of the academy or the Focus-Trust.

Personal use of Social Media

Staff members must not identify themselves as employees of the academy or Focus-Trust or service providers for the academy or Focus-Trust in their personal webspace. This is to prevent information on these sites from being linked with the academy and the Focus-Trust and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

Staff members must not have contact through any personal social medium with any pupil, whether from the academy or any other academy, unless the pupils are family members.

The academy does not expect staff members to discontinue contact with their family members via personal social media once the academy starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

Staff members must not have any contact with pupils or pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity or suitability.

Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts. Instead, if they receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become 'friends' of the official academy site.

On leaving the academy service, staff members must not contact the academy pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former academies or schools by means of personal social media.

Information staff members have access to as part of their employment, to personal information about pupils and their family members, colleagues, and other parties and academy or Focus-Trust corporate information, this must not be discussed on their personal webspace.

Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing academy or Focus-Trust uniforms or clothing with academy or Focus-Trust logos or images identifying sensitive academy or Focus-Trust premises (eg care homes, secure units) must not be published on personal webspace.

The Academy or Focus-Trust email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

The academy or Focus-Trust corporate, service or team logos or brands must not be used or published on personal webspace.

The academy only permits limited personal use of social media while at work. Access to social media sites for personal reasons is only allowed during lunch breaks. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the academy's time.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Using social media on behalf of the academy or Focus-Trust.

Staff members can only use official academy sites for communicating with pupils or to enable pupils to communicate with one another.

There must be a strong pedagogical or business reason for creating official academy sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the academy to unwelcome publicity or cause reputational damage. Central approval must be sought.

Official academy sites must be created only with the approval of the Trust central administration team. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

Monitoring of internet use

Focus Trust and the academy will monitor usage of its internet and email services without prior notification or authorisation from users.

Users of email and internet services across the Trust should have no expectation of privacy in anything they create, store, send or receive using the academy's IT system.

Breaches of the guidance

Any breach of this guidance may lead to disciplinary action being taken against the Staff member/s involved in line with the Focus-Trust Disciplinary Guidance and Procedure.

A breach of this guidance leading to breaches of confidentiality, or defamation or damage to the reputation of the academy or the Focus-Trust or any illegal acts or acts that render the academy or the Focus-Trust liable to third parties may result in disciplinary action or dismissal.

Contracted providers at any of the academies or Focus-Trust services must inform the relevant academy or Focus-Trust officer immediately of any breaches of this guidance so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the academy and the Focus-Trust. Any action against breaches should be according to contractors' internal disciplinary procedures.