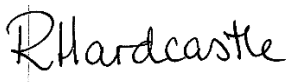
Hatton Academies Trust

Title	**E-Safety & Acceptable Use Policy**
Reviewed	**March 2019**
Next Review	**September 2020**
Associated Policies	**Mobile Device Policy** **Behaviour Policy** **Anti-Bullying Policy** **Child Protection Policy**
Originator	**V Bishop/R Chambers**
Approved	

Contents

E-Safety Policy for Hatton Academy Trust

1. E-Safety Defined

"The trust's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate".

There are considered to be 3 main areas of risk with regards to E-Safety for children:

1. Being exposed to illegal, inappropriate or harmful material.

2. Being subjected to harmful online interaction with other users.

3. Personal online behaviour that increases the likelihood of, or causes, harm."

Hatton Academies Trust has measures and procedures to our statutory responsibilities as outlined in:

Computer Misuse Act 1990
Specifies that any person who accesses another user's account even to look at their files is breaking the law and is guilty of accessing materials without authorization. Other offences include accessing another user's account and modifying materials. It is against the law to access a person's account and make changes. Further to this, it is also illegal to write a program which may cause disruption to any users' computer or account.

Malicious Communications Act 1988
Specifies that any person who sends an electronic communication which conveys a message which is indecent or grossly offensive, a threat, or information which is false and known or believed to be false by the sender, is guilty of an offence if their purpose in sending it was to cause distress or anxiety to the recipient

Children Act 1989
If there is 'reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm' the incident should be addressed as a child protection concern. School staff should discuss with the school's designated safeguarding lead and, where appropriate, they will report their concerns to their local authority children's social care and work with them to take appropriate action. Where there is no reasonable cause to suspect the suffering or the likelihood of suffering significant harm schools may need to draw on a range of internal and external services to support the pupil who is experiencing bullying, or to tackle any underlying issue which has contributed to a child engaging in bullying

The Education and Inspections Act 2006
Section 89 provides that maintained schools must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents.

The Equality Act 2010
A key provision is the Public Sector Equality Duty (PSED), which came into force on 5 April 2011 and covers age, disability, gender reassignment, pregnancy and

maternity, race, religion or belief, sex and sexual orientation. It requires public bodies to have due regard to the need to:

- eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Act
- advance equality of opportunity between people who share a protected characteristic and people who do not share it
- foster good relations between people who share a protected characteristic and people who do not share it.

The Education Act 2011
Amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized by a member of staff who has been formally authorised by the head teacher, that staff member can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

The Education (Independent School Standards) Regulations 2014
The proprietor of an Academy or other independent school ensures that bullying at the school is prevented in so far as reasonably practicable, by the drawing up and implementation of an effective anti-bullying strategy.

Keeping Children Safe in Education Guidance 2018.

2. What is an E-Safety Policy?
Internet technology helps pupils learn creatively and effectively. It encourages collaborative learning and the sharing of good practice amongst all Trust stakeholders from staff, learners, directors,through to parents/carers. This E-Safety policy encourages appropriate and safe conduct and behaviour during this process.

The positive effects of the policy are intended to be seen online and offline in our academies and at home, and ultimately beyond the trust and into the community and the workplace.

Pupils, staff and all other users of trust related technologies work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour and safe E-Conduct. They do this through a variety of meetings including between members of the peer team and the guidance/pastoral team.

These agreements and their implementation promote positive behaviour within the Trust Academies. This policy is not designed to be a blacklist of prohibited activities; it is a list of areas to discuss, teach and inform. It will develop positive behaviour and knowledge leading to safer internet use and year-on-year improvement, with a measurable impact on E-Safety.

3. E-Safety Policy - Scope

This policy and the agreements herein apply to all pupils, staff, support staff, external contractors and members of the Hatton Academies Trust community who use, have access to, or maintain Trust and academy-related internet and computer systems internally and externally.

The Trust will make reasonable use of relevant legislation and guidelines to effect positive behaviour regarding ICT and internet use on and off the Trust sites. This will include the use of rewards and sanctions for inappropriate behaviour as defined as 'regulation of student behaviour' under the Education and Inspections Act 2006 and in the individual school behaviour policies. Under the Children Act 1989 the Trust can report and act upon instances of cyber-bullying, abuse, harassment, malicious communication and grossly offensive material. This includes reporting to the police, social media websites, and hosting providers on behalf of pupils and their parents/carers.

This policy covers the use of (also see the Mobile Devices Policy):

- Mobile phones when used on Trust sites
- Pupils' and staff's personal ICT equipment when used in our academies and which makes use of Trust networking, file-serving or internet facilities.
- External access to internal Trust networking such as email, remote access and printing etc.
- Trust related external internet including, but not limited to learning platforms, blogs, social media websites.
- Trust based ICT systems and equipment including PC's, laptops, netbooks, i-pads etc.

4. Ensuring Good Practice

The E-Safety policy results from a cycle of evaluation and review based upon new initiatives and discussion with stakeholders and outside organisations, technological and internet developments, current Government guidance and Trust, county advisor and police related E-Safety incidents.

The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum.

The policy is rewritten / amended annually for ratification by the CEO on behalf of the Directors. Regular assessment of strengths and weaknesses helps to determine inset provision for staff and directors and guidance for parents/carers, pupils and local partnerships.

Additionally, the policy and training needs will be reviewed promptly upon:

- Advice from the police
- E-Safety incidents in the local community or local academies which might impact on the Hatton Academes Trust community

- Significant changes in technology as used by the trust or pupils in the wider community
- New guidance by Government/LEA/safeguarding authorities
- Serious and/or frequent breaches of the acceptable internet use policy or other in the light of E-Safety incidents.

E-Safety is taken very seriously by Hatton Academies Trust for example it is the focus of activities, assemblies and training (student and staff) etc.

Furthermore E-Safety is timetabled into staff training days to ensure that all staff are fully aware and up to date in terms of E-Safety for both themselves and for the learners in their care (the training is undertaken based upon staff training needs as indicated by questionnaires, the responses to training etc.).

A number of members of staff have received accredited associated training over the last two years.

Pupils, parents/carers, wider academy community stakeholders and directors all contribute to build a fluid and constantly evolving E-Safety policy.

Procedures for monitoring, logging, reporting incidents, evaluating, improving and measuring the impact of E-Safety are in place. All staff, parents/carers, pupils, contractors and directors know how to report any E-Safety incident, through written/ verbal information, the school websites and the behaviour, acceptable use, mobile devices and anti-bullying policies (as applicable).

4.1 Filtering

We have changed the ISP for the Trust, we are running:

- A “next-generation” filtering program (Surfprotect Quantum from Exa-Networks).
- Fortinet as the firewall
- Netsupport which supports new browser technology such as Edge.
- Sophos email filter.
- Safe search for search engines (part of the web filter that we use).

5. In the Event of an E-Safety Incident

All E-Safety incidents are recorded via Trust/academy systems. These are reviewed daily by staff and are analysed formally on a regular basis. All Trust academies continue to develop their recording systems for incidents.

Any incidents where members of the Trust community (staff, students etc.) do not follow the Acceptable Use Policy are dealt with following the academy trust’s normal behaviour / disciplinary procedures.

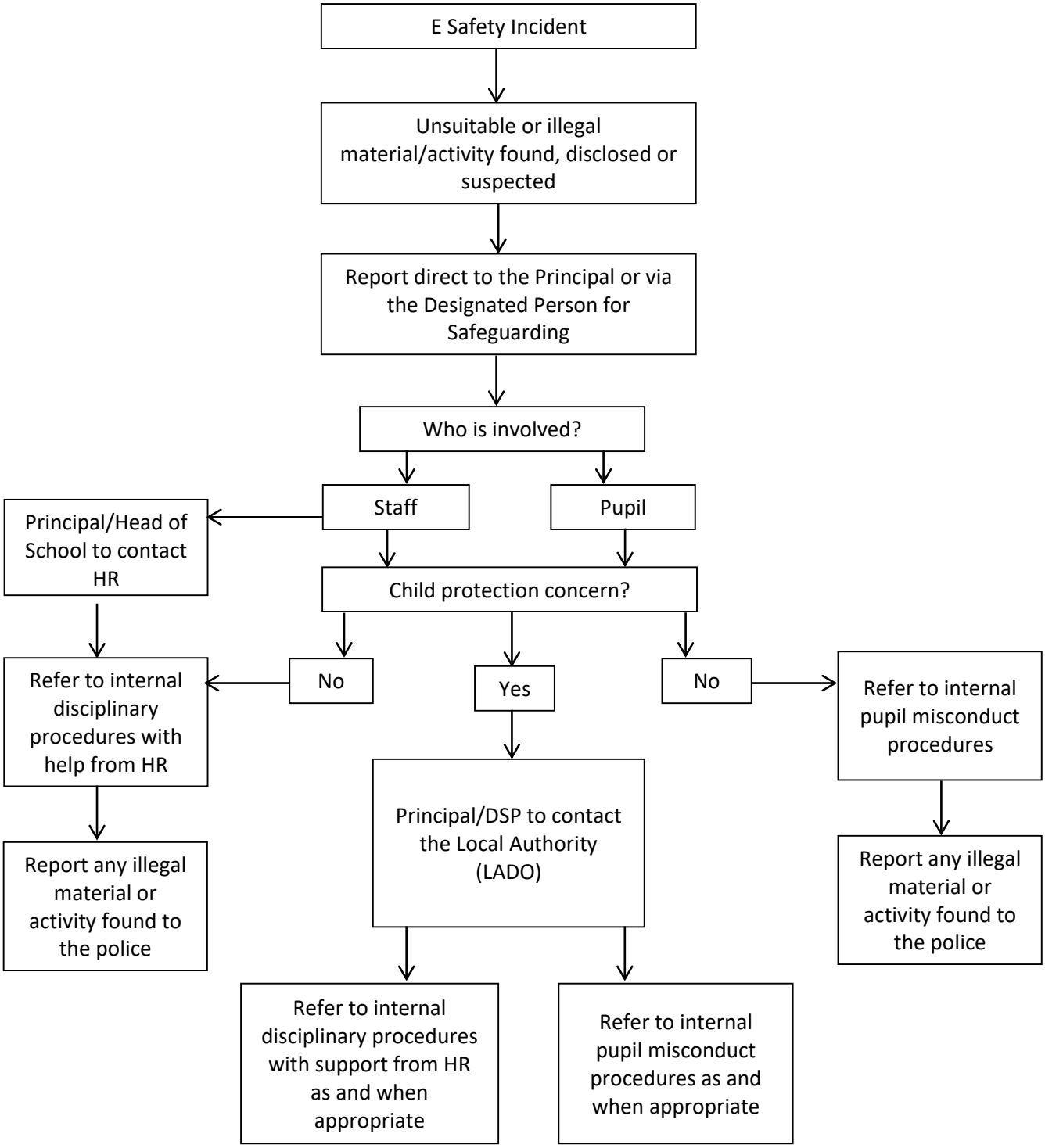
Where a member of staff is made aware of any incident, concerning students/pupils (or staff), they inform a designated person (for E-Safety) or the DSL, their line manager and/or Head of School/Principal directly (also recording the incident e.g. on

the individual school's reporting systems, who will then respond in the most appropriate manner).

All instances of bullying, including cyber-bullying are taken very seriously by Hatton Academies Trust and are dealt with using the individual academies anti-bullying / behaviour procedures. The Trust recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

As a Trust we reserve the right to monitor equipment (e.g. using NetSupport software) on the premises and to search any technological equipment, including personal equipment with permission, when a breach of this policy is suspected. (All searches being carried out in accordance with the relevant policies)

Incidents which create / suggest a risk to the security of the Trust networks, or create / suggest an information security risk, will be referred to the designated person (for E-Safety) and technical support (appropriate advice may be sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance) within that setting. If there have been breaches of academy policy then appropriate sanctions will be applied. The academy will decide if parents/carers need to be informed.


E Safety Incident
Unsuitable or illegal material/activity found, disclosed or suspected
Report direct to the Principal or via the Designated Person for Safeguarding
Who is involved?
Staff
Pupil
Principal/Head of School to contact HR
Child protection concern?
Refer to internal disciplinary procedures with help from HR
No
Yes
No
Refer to internal pupil misconduct procedures
Report any illegal material or activity found to the police
Principal/DSP to contact the Local Authority (LADO)
Report any illegal material or activity found to the police
Refer to internal disciplinary procedures with support from HR as and when appropriate
Refer to internal pupil misconduct procedures as and when appropriate

6. Policy Review Schedule and Evaluation

The designated person for E-Safety within the setting will liaise with stakeholders across Hatton Academies Trust. There will be an annual review (in the summer term) as part of the Trust Safeguarding Meeting, to monitor and evaluate the policy and its effectiveness. The review committee will comprise:

- CEO
- Trust E-Safety Co-Ordinator
- Academy Principal
- DSL's Designated Senior Leaders for each trust academy
- E-Safety co-ordinator (academies)
- HAT Network manager
- Representatives of Board of Directors
- Representative of teaching staff

The HAT E-Safety Co-ordinator will seek parent and pupil feedback on the effectiveness of our policy and procedures.

In the event of an incident, the following people will be informed within the academy and in external agencies and stakeholder organisations:

- The Designated Person for Anti-Bullying/E-Safety
- DSL
- Pastoral heads and potentially the police
- CEOP and/or service providers
- Relevant academy senior leaders.

7. Roles

7.1 Trust and Academy Level Management of E-Safety

The Principal in each Trust Academy is responsible for the implementation of this policy and will contribute to the evaluation of its effectiveness. This evaluation includes teaching and learning, use of academy trust IT equipment and facilities by pupils, staff and visitors. It also includes agreed criteria for the acceptable use by students, pupils, academy trust staff, Directors and Academy Representatives of internet-capable equipment for academy trust related purposes and the training prepared to staff and pupils / the curriculum delivery.

At Hatton Academies Trust our E-Safety provision is always designed to encourage the use of the internet and positive behaviours and practical real-world strategies for all members of the academy and wider academy community.

7.2 The Academy "E-Safety Designates"

Each academy designated E-Safety Representative reports to the senior team and Principal (CEO) and co-ordinates E-Safety provision. They liaise with senior leaders and the academies Designated Safeguarding Lead and other senior leaders as required.

Although all members of the Trust community (staff, students, and directors) are responsible for upholding the academy Trust E-Safety policy, the E-Safety designates, the Designated Safeguarding Lead and ICT support are responsible for monitoring internet usage by pupils and staff, and on academy machines, such as laptops, used off-site (see the Mobile Devices and Behaviour policies).

The E-Safety leads are responsible for promoting best practice in E-Safety, including providing and being a source of information for parents/carers and partner stakeholders.

The Sir Christopher Hatton/Trust E-Safety Coordinator attends the Safeguarding Committee which includes representatives of the academy community including relevant local stakeholders to ensure at least annual monitoring and evaluation of our e-safety monitoring and procedures. E-safety is a standing item on the Trust Safeguarding Committee agenda.

The Trust academy e-safety leaders will produce an annual report for the CEO and Board of Directors.

E-Safety designates are responsible for responding to E-Safety issues on a day to day basis.

The E-Safety designates audit (e.g. through questionnaires (e.g. the E-Safety audit at SCHA) and feedback from students during peer team meetings etc.) and assesses inset requirements for the Trust community, and ensures that all staff are aware of their responsibilities and the Trusts E-Safety procedures. The coordinator is also the first port of call for staff requiring advice on E-Safety matters.

8. Director's Responsibility for E-Safety

The Board of Directors will be informed of the review committee findings and have E-Safety as an annual agenda item for their input.

The E-Safety Designates/Coordinator will ensure that Directors are informed of E-Safety requirements.

9. ICT Support Staff and External Contractors

All staff are required to sign an acceptable user agreement upon receiving their log-in information and any laptops etc.

ICT support-staff are responsible for the Trusts IT network, infrastructure and hardware. They ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.

Support staff will maintain and enforce the Trust password procedures and are strictly prohibited from sharing their log in information (as are students and pupils)

External contractors, such as website providers, website designers etc. are made fully aware of and agree to the Trust's E-Safety Policy. Where contractors have access to sensitive academy information and material covered by the Data

Protection Act, for example on a VLE, Trust websites or email provision, the contractor is CRB/DBS checked.

10. Teaching and Support Staff

Teaching and support staff will be provided with E-Safety induction as part of the overall staff induction procedures, this is registered and logged.

Teaching and support staff are aware of the current Trust E-Safety policy, practices and associated procedures for reporting incidents through training, access to the policy and updates during staff training.

Regular training occurs with all staff (including teachers, support and ancillary staff) being required to attend. Any staff that are not present are required to attend further training sessions at a later date. Registers are taken so that attendance can be logged and monitored, and staff sign and submit a user agreement sheet which is then logged by HR. Staff are also required to undertake online training in E-Safety annually.

All staff are expected to have read, understood and signed (thereby indicating an agreement) the Acceptable Use Policies relevant to internet and computer use in academy trust guidance (Appendix 2).

All staff are required to follow the Trust's social media guidance (Appendix 1), in regard to external off site use, personal use (mindful of not bringing the trust into disrepute), possible contractual obligations, and conduct on internet academy messaging or communication platforms. (See the Mobile Devices Policy).

All teaching staff must monitor pupil internet and computer usage in line with the policy (both physically and, where applicable, through software e.g. NetSupport). This also includes the use of personal technology such as cameras, phones and other gadgets on the academy site (also see the Mobile devices policy).

Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism. (Audited through the Departmental E-Safety Audit at SCHA Feb 2018)

During trips and visits, staff are to use the Trust's mobile phones rather than their own and furthermore they must not have the mobile phone numbers of a student or share theirs with a pupil.

Staff **must not** make "friends" or otherwise connect with students through social media and are advised not to post content which could put both staff and students reputation at risk or bring the reputation of the Trust into disrepute.

It is strongly recommended that staff should not have ex-students or siblings of current students as "friends "on any social media platform. The exception is when ex-students have been left long enough ie. Over 25 years old or are not connected in any way with a trust academy.

All staff will maintain and enforce the password policy and are strictly prohibited from sharing their log in information. Student passwords can be subject to forced change at no notice if justified by events.

All staff must agree and sign the HAT E-Safety acceptable use agreement (Appendix 2). These are to be shared with staff via paper copies in their pigeon holes and an agreement to comply form is returned, by staff, for collation.

11. Designated Safeguarding Leads (DSL)

The DSL is trained in specific E-Safety/child protection issues.

The DSL differentiate which E-Safety incidents are required to be reported to CEOP, local Police, social services and parents/carers etc.

Possible scenarios might include (see the Anti-bullying and mobile devices policies):

- Allegations against members of staff.
- Computer crime – for example hacking of Trust systems.
- Allegations or evidence of 'grooming'.
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment, the distribution or creation of inappropriate images of minors: or a malicious communication.

Where necessary they will liaise with websites and social media platforms such as Twitter and Facebook to remove illegal material or cyber bullying.

There are established reporting streams and training is given during staff training days regarding the reporting of concerns, e.g. at SCHA through CPOMS.

12. Pupils/Students

Pupils/students are required to use Trust internet and computer systems in agreement with the terms specified in the Acceptable Use section of this policy. This is summarised in student planners or for primary age pupils it forms part of the Home-School Agreement.

Parents and carers are expected to sign the policy to indicate agreement at SCHA. This covers all computer, internet and gadget usage in academy, including the use of personal items such as phones.

Pupils/students (and staff) are to report E-Safety incidents which are monitored, at SCHA by the E-Safety Coordinator, and are reported on half termly (and through external reporting facilities, such as the CEOP report abuse button as appropriate). This is ensured through teaching during curriculum and pastoral time.

Pupils/students will maintain and enforce the Trust's password policy and are strictly prohibited from sharing their log-in information.

Pupils/students must understand that their internet use out of their academy on social networking sites such as Facebook is covered under the Acceptable Use

section if it impacts on the Trust and/or its staff and pupils as cyber bullying, reputation or illegal activities (including youth produced sexual imagery).

13. Parents and Carers

It is expected that parents/carers will support the Trust's stance on promoting good internet behaviour and responsible use of IT equipment both at their academy and at home.

Hatton Academies Trust expects parents and carers to sign the Trust's Acceptable Use Policy, indicating agreement regarding their child's and their own use of academy systems such as the academy website etc.

The Trust will provide opportunities to educate parents with regard to E-Safety (E.g. during Anti-bullying and E-Safety week).

14. E-Safety Education

Behaviours which will be highlighted include (some dependent on setting):

- The medical and social effects of spending too much time on the internet, games consoles or computers
- Explaining why harmful or abusive images on the internet might be inappropriate or illegal. (Incidents where students have sent or disseminated images of minors (sexts/sexting/ youth produced sexual imagery) will be recorded on a referral from and handed directly to a DSL who would refer it to external agencies
- Encouraging responsible and effective digital literacy skills which extend beyond academy and into the workplace
- Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe and may result in prosecution
- Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal
- Teaching why certain behaviour on the internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal activities such as grooming and sexting can develop
- Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it

- Teaching pupils to assess the quality of information retrieved from the internet, including recognising how reliable, accurate and relevant information is – particularly information obtained from search engines.
- Informing pupils and staff of copyright and plagiarism infringement laws, and potential consequences with regard to copying material for homework and coursework, copying photographs and images on social networking sites, copying material for using in teaching materials, downloading music, video, applications or other software files illegally.

15. To Pupils/Students

E-Safety is delivered through:

- Teaching units/Lifeskills etc.
- Pastoral care
- E-Safety events – such as Anti Bullying Week and E- Safety Week
- Online training – including online training

16. To the Wider Trust Community /Stakeholders

E-Safety information goes to parents/carers through planners, newsletters, learning platform, website etc.

Parents Evenings, open days, transition evenings may also be used

Twilight presentations run by the Trust for parents/carers and wider academy community stakeholders e.g. during Anti Bullying Week and E-Safety Week at Sir Christopher Hatton.

17. Staff and Directors

E-Safety training is delivered to staff through training day presentations, emails etc. resources etc. including online training. It is for each academy to determine and deliver training for their staff. The trust will deliver whole Trust training as appropriate and evaluate effectiveness through the Trust E-Safety meeting.

INSET opportunities to be made available for staff, including on site inset, whole staff training, online training opportunities (for example through Stonewall, NSPCC, E-Safety advisor and the Anti-Bullying alliance).

Directors will be invited to staff training events and other training will be organised as required.

The E-Safety policy is updated and evaluated by staff each academic year at the annual meeting.

The E-Safety designate should be the first port of call for staff requiring E-Safety advice.

18. Data Protection

The Trust recognises their obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

Pupils/students are taught about the need to protect their own personal data as part of their E-Safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are aware of their obligation to keep sensitive data secure when working on computers outside academy
- Laptops are also encrypted for protection
- Staff are encouraged to use the Trusts Office 365 implementation for online storage for their data. Office 365 is GDPR & Data Protection Act 2018 compliant as long as the users password is secure.
- All computers or laptops holding sensitive information are set up with strong passwords and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the Trust management information systems holding pupil data. Passwords are not shared and administrator passwords are kept securely
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for academy data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example Directors, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies
- We do not distribute memory sticks, apart from the ones that the DSL uses, these are encrypted
- The laptops of the pastoral teams are encrypted due to the sensitive / confidential nature of the work that is stored / accessed via them

- Mobile devices that staff connect to the e-mail server are pass-coded and our Exchange server controls them so that if those devices were lost or stolen the user can log into their webmail and erase their device.

- Staff should ensure that the mobile device is encrypted as well.

19. Acceptable Use

19.1 Staff

The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal):

Training is part of staff induction.

- Accessing inappropriate or illegal content deliberately

- Deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent

- Sending or posting material regarded as harassment, or of a bullying nature (after being warned)

- Using digital communications to communicate with pupils or meet ex-pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones) (staff may not have/store students mobile phone numbers etc.), or communication via social networking sites

- Using personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission

- The transportation of confidential material from one location to another unprotected by encryption. Staff must follow academy data security protocols when using any such data at any location. Staff and / or pupil information, e.g. reports, SIMS data etc. must be kept private and confidential, EXCEPT when it is required by law to disclose it.

- The projection of staff emails (as students could see confidential material).

The following activities are likely to result in disciplinary action:

- Any online activity by a member of the Trust community which is likely to adversely impact on the reputation of the academy

- Accessing inappropriate or illegal content accidentally and failing to report this

- Leaving a laptop / computer unsupervised and accessible to students (not shut down and/or password protected)

- Inappropriate use of personal technologies (e.g. mobile phones) (see Mobile devices policy)

- Sharing files which are not legitimately obtained e.g. music files from a file sharing site
- Using Trust or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the academy trust into disrepute

- Using email and other systems to avoid proper following of trust policies and procedures.

- Attempting to circumvent Trust filtering, monitoring or other security systems

- Circulation of commercial, advertising or 'chain' emails or messages

- Revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission

- Using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)

- Transferring sensitive data insecurely or infringing the conditions of the Data protection Act 2018.

The following activities would normally be unacceptable; however in some contexts they may be allowed e.g. as part of planned curriculum activity or as system administrator to solve a problem:

- Accessing social networking sites, instant messaging accounts, email or using a mobile phone etc. for personal use during lesson time

- Accessing non-educational websites (e.g. gaming or shopping websites) during lesson time

- Sharing a username and password with others or allowing another person to log in using your account

- Accessing Trust ICT systems with someone else's username and password

- Deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Furthermore staff must:

- Be aware of and comply with the entirety of this policy document

- Use the academy website / learning platform in accordance with the acceptable use policy

- Ensure the secure storage of confidential student data e.g. when printed such as for report checking or an observation, they must be kept securely / shredded

- Ensure that any private social networking sites / blogs etc. that they create or contribute to are not confused with their professional role

- Not download any software or resources from the Internet that can compromise the network, or are not adequately licensed

- Embed E-Safety curriculum into their curriculum

- Alert the individual academy's named DSL / relevant senior member of staff if they feel the behaviour of any child I teach may be a cause for concern (e.g. in the event of suspected youth produced sexual imagery being made, sent or shared)

- Understand that all Internet usage, email and network usage can be logged and this information could be made available to the CEO on request. All staff sign the Acceptable User Agreement.

- Report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / academy named contact

- Understand that it is their duty to support a whole-academy trust safeguarding approach and will report any behaviour (by any person), which they believe may be inappropriate or concerning in any way, to the anti-bullying /E-Safety coordinator or child protection officer at the academy

- Not publish or distribute work that is protected by copyright

- Understand that failure to comply with this agreement could lead to disciplinary action

20. Pupils/Students

20.1 Defining "misuse"

The Trust Internet, website, email and related technologies must not be used for knowingly viewing, transmitting, retrieving, downloading or storing anything that is:

- Obscene or pornographic

- Discriminatory, derogatory or harassing

- Defamatory, threatening or seen as cyber-bullying
- Illegal or contrary to academy policies / interests
- Subject to copyright e.g. music, software or films.

Students must comply with the entirety of this document

Pupils / students also must not:

- Use mobile devices or other technologies to store or upload such materials to social networking sites etc. or to other devices
- Play web based games, unless directed by their class teacher (who will ensure that they are appropriate)
- Use mobile phones or other digital technologies during lessons unless at the express direction of the classroom teacher (sanctions as per each school policy)
- Use mobile phone cameras or digital cameras in their academy unless directed to by a member of staff
- Use cameras/phones to record Trust staff and other students
- Use the academy email during lessons unless directed to by the teacher
- Deface or otherwise damage trust equipment
- Load files or use them files to gain access to unauthorised areas of the network
- Access another user's area
- Tamper or gain/attempt to gain access to unauthorised areas of the academy network.
- Access other students work without permission by a member of staff or the student whose work it is
- Change the settings of computers/laptops etc. for example screen displays; desktop images

- Use USB drives or any removable storage devices unless they have been checked for viruses.

Appendix 1 (Also see the Mobile devices policy)

Detailed guidance on the use of Social Media for:
Staff

- Staff must adhere to (and agree to adhere to) Hatton Academies Trust's policies with regards to acceptable use, social networking, behaviour and anti-bullying

- Photographic material and/or video footage that include pupils must NOT be taken using PERSONAL equipment (e.g. mobile phones, i-pads, tablets or camcorders) unless with permission from a line-manager. Any recorded material must then be saved onto the trust's networks and then be deleted from the staff equipment

- Remember posts/tweets/blogs are an extension of your classroom, what is inappropriate in the classroom is also deemed inappropriate online

- Any posts etc. that you make should portray you in a professional manner, remember that students and parents/carers and other stakeholders may see what you post

- Always make sure that you log out of Facebook etc. after using it, particularly when using a machine that is shared with other colleagues/students. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off

- There should be no tagging of other staff without their permission

- Pupils must NOT be in any photograph that is uploaded

- Staff must not post confidential information about students, staff or the trust

- The use of profanity or threatening language is forbidden

- Under no circumstances should negative comments be made about students, Parents/carers, other staff or the Trust

- Be respectful of the opinions of others in your posts or comments

- Do not post personal information about yourself, current or past members of staff
- When posting opinions please remember that you are still representing the Trust to the wider community.

- Passwords and other login information must remain strictly confidential at all times and kept secure. If you feel that your password is no longer secure, reset it

- Staff should communicate with students through the academy email system, and not through personal accounts, as outlined in the Acceptable Use Section

- Friending/following/liking current student's personal accounts are strictly forbidden

- Staff are advised to ensure that their privacy settings of their personal social media accounts / pages are limited to 'friends'

- Respect brand, trademark, copyright information and/or images of the school

- When using hyperlinks, be sure that the content is appropriate. Always check where they take you (and any other links from there) before you share it

- Staff should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online, plagiarism must be avoided

- Staff are advised to carefully consider whether to use a dating app due to the personal nature of conversations which can occur on these. Staff are asked to consider their security and be fully aware of who they're talking to.

- Staff are discouraged from using images of themselves as "profile images" or their real names on their profile.

The Trust reserves the right to monitor employees' internet usage, but will endeavor to inform an affected employee when this is to happen and the reasons for it.

The Trust considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been spending an excessive amount of time viewing websites that are not work-related

- acted in a way that damages the reputation of the Trust and/or breaches confidentiality.

Hatton Academies Trust reserves the right to retain information that it has gathered on employees' use of the internet.

If the Trust monitors employees' internet use to ensure that it is in accordance with this policy, access to the web may be withdrawn in any case of misuse of this facility.

If appropriate, disciplinary action may also be taken in line with the Trust's Disciplinary Policy. In serious cases e.g. of harassment or cyber bullying or in breaches of confidentiality this may be treated as Gross Misconduct and the employee may be summarily dismissed.

Guidelines for Students and pupils

- Students must adhere to (and agree to adhere to) the Trust's policies and guidance with regards to acceptable use, social networking, behaviour and anti-bullying

- Any instances of cyber-bullying will be dealt with (through the anti-bullying and behaviour policies) promptly, regardless of the source of the issue

- Students shall continue to adhere to the Trust's policies on use of personal data

- Students are expected to, and must adhere to, terms and conditions of use (including age restrictions) as agreed when they sign up to Facebook, Twitter, Pinterest, Snapchat, or any of the other social media platforms

- Students may not post photos of students / staff or tag students / staff without their permission

- Do not engage in any abusive, threatening, unkind or bullying behaviour of staff, parents or of other students. The use of profanity or threatening language is also forbidden

- Your online behaviour should reflect the same standards of honesty, respect and consideration that you are expected use face-to-face this includes the use of homophobic and disabilist language for example. Be respectful of the opinions of others in your posts or comments

- Students are advised to ensure privacy settings of their personal social media accounts / pages are limited to 'friends' and that they do not accept any "friend" that they cannot verify as an existing friend or acquaintance

- Passwords and other login information must be confidential at all times and be kept secure. If you feel that your passwords are no longer secure, get them reset

- Unless otherwise stated by teachers or other staff, use of social media shall not be permitted during classroom hours. The Trust reserves the right to confiscate electronic devices if used inappropriately during lessons.

- Users should not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online, plagiarism is traceable and can result in sanctions

- Current students or those with siblings that are current students may not attempt to “friend” any member of Trust staff

- Research conducted via the Internet should be appropriately cited, giving credit to the original author

- Any instances of cyber-bullying must be reported to the anti-bullying designate as soon as possible, even if you have already reported it through an internet security “button”.

Guidelines for Parents and carers

- The Trust is not responsible for improper use of social media by students. It is the responsibility of parents/carers to monitor their child’s activities on social media

- Parents/carers must not use profanity or engage in any abusive, threatening or bullying behaviour. Under no circumstances should negative comments be made about students, staff or other parents through Social Media by students or their parents/carers

- Please do not post photographs of other pupils without securing permission from their parents / carers first

- Parents may not “friend” staff working for the Trust.

Appendix 2

Hatton Academies Trust Acceptable Use Policy (AUP) 2018:

Staff Agreement Form

I agree to abide by all the points in the document above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the Hatton Academies Trust's most recent E-Safety policies.

I wish to have an email account; be connected to the Intranet / Internet; be able to use the academy's ICT resources and systems.

Signature ..... ….Date.....

Full Name ..... (printed)

Job title .....

HAT Academy .....

Appendix 3

E-Safety/ Acceptable use policy 2018 (student)

Guidelines for pupils

- Pupils must adhere to (and agree to) the academy trust's policies for acceptable use, social networking, behaviour and anti-bullying.
- Any instances of cyber-bullying will be dealt with promptly, regardless of the source of the issue.
- Pupils are expected to, and must adhere to, terms and conditions of use (including age restrictions) as agreed when they sign up to Facebook, Twitter, Pinterest, or any of the other social media platforms.
- Pupils may not post photos or videos of other students or tag other pupils without their permission (see the anti-bullying, E-Safety and mobile devices policies), there must be no images (photos or video) taken in school by pupils.
- Do not engage in any abusive, threatening, unkind or bullying behaviour of staff, parents or of any other pupils online. This includes the use of homophobic or disabilist language for example. Be respectful of the opinions of others in your posts or comments.
- Pupils are advised to ensure that their privacy settings of their personal social media accounts/pages are limited to "friends".
- Passwords and other login information must be confidential at all times and be kept secure. If you feel that your passwords are no longer secure, get them reset.
- Unless otherwise stated by teachers or other staff, use of social media shall not be permitted during classroom hours. The academy trust reserves the right to confiscate electronic devices if used inappropriately during lessons.
- Users should not take credit for things that they did not create themselves, or misrepresent themselves as an author or creator of something found online, plagiarism is traceable and can result in sanctions.
- Student must not use academy devices inappropriately, any inappropriate searches etc. can be recorded and sanctioned by the academy.
- Pupils may not "friend" any member of academy trust staff
- Any instances of cyber-bullying must be reported to the Anti-bullying Coordinator soon as possible, even if you have already reported it through an internet security "button".
- Students are responsible for anything that occurs when they are logged in. They must log out of / or lock any computer that they are logged into in the event of them leaving it unattended.
- Pupils may not post or share any explicit images of themselves or others

I have read and understand the above and will abide by these points

Signed (pupil): _____

_____

Date: _____

Signed (parent): _____

Date: _____

E-Safety and Internet – Use of Good Practice Policy

The trust and each trust encourages the safety and appropriate use of ICT.

Policies are in place to maintain safety and ensure that facilities and services are used for the purpose of enhancing learning .

Please complete and sign below

Pupil name:

……

……

I have read and understood the trust's E-Safety / acceptable use policy. I will use the computer system and internet in a responsible way and obey the rules at all times. I understand that the full, current, updated policy is available on the school website.

Signed:

……

……

Parent/Carer's Consent for Internet Access

I have read and understand the academies E-Safety and acceptable use policy and give my permission for my son/daughter to access the Internet. I understand that the trust and the academy will take reasonable precautions to ensure that pupils cannot access inappropriate materials. I also understand that the academy/trust cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the trust/academy is not liable for any damage arising from the use of the internet facilities. I accept that the full current policy applies and that updated versions are available on the website.

Parent/Carer name:……

……..

Parent/Carer signature:……

.....Date:……