




Online safety policy

Document Control

Description	By Whom	Date
Established (from previous data protection and e-safety policy)	WM	Mar 2020
Reviewed	SP / DB / WM	Apr 2024
Approved by ELT	 A Hughes CEO	May 24
Next Full Review due		May 26

Contents

1. Aims	4
The 4 key categories of risk.....	4
Online Technology includes a wide variety of devices	4
Right to Online Access	4
2. Legislation and guidance	5
3. Roles and responsibilities (these lists are not intended to be exhaustive)	5
The Board of Trustees.....	5
Executive Principals/ Principals/ Heads of Academy.....	5
The Designated Safeguarding Lead.....	5
Head of IT and IT infrastructure manager	6
Academy Online Safety Group	6
All staff and volunteers, including agency staff, contractors, students, and volunteers.	6
Parents/ Carers	6
Visitors and members of the community	6
4. Educating pupils about online safety	7
5. Educating parents about online safety.....	7
6. Cyber-bullying.....	7
Definition	7
Preventing and addressing cyber-bullying.....	7
Examining electronic devices	8
Artificial intelligence (AI)	8
7. Acceptable use of the internet in the Academy/ Trust	9
Staff:.....	9
Early Years Foundation Stage Pupils:.....	9
Key Stage 1 and 2 Pupils	9
Other children visiting an Academy	9
Professionals.....	9
Parents.....	9
All Users.....	10
8. Pupils using mobile devices in school	10
9. Pupils using Trust devices outside of school	10
10. Staff using work devices outside school	10
11. How the Trust/ Academy will respond to issues of misuse	10
12. Training	11
13. Filtering and Monitoring arrangements	11
15. Links with other policies.....	11
15. Equality Impact Assessment.....	11
16. Data Protection Statement	12
Appendix 1: EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers).....	13
Appendix 2: KS2 acceptable use agreement (pupils)	14
Appendix 4 : KS2 Terms and Conditions for use of Electronic Equipment (parents/carers)	16
Appendix 5: Acceptable Use Agreement (Staff, Trustees, Volunteers, Students and Visitors).....	17
Appendix 6: Online safety training needs – self-audit for staff.....	18
Appendix 7: Senso Security Data Sheet.....	19

Appendix 8: Online Safety Policy Review and Audit - Academies to Complete.....20

1. Aims

The online safety policy aims to outline safe and effective practice specific to the use of the internet. It provides advice on acceptable use and effective measures to enable children and adults to use the internet in a safe way.

This policy applies to all individuals who have access to and/or are users of work-related internet systems. This includes (but is not exhaustive):

- children
- parents and carers
- staff
- Trustees
- practitioners and their managers
- volunteers
- students
- committee members
- visitors
- contractors
- community users

Our Trust/Academies aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, Trustees, and other appropriate adults.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy forms part of the Trust's strategy on **Harnessing Technology, Maximising Learning** (HTML).

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual, and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Online Technology includes a wide variety of devices

Online Technology encompasses a wide range of media applications and connecting methods which are continually changing and advancing. These include, but are not limited to:

- Computers, laptops, iPad's, tablets, smart TVs – access to fixed and mobile internet, email, chat rooms, blogs, social networking sites, podcasts, instant messaging, and location-based technologies.
- Wireless and Broadband access,
- Mobile phones with internet access, Bluetooth, cameras, videos, Wi-Fi and more,
- Gaming – online and game consoles, many of which can be interconnected with other devices,
- Video broadcasting and music downloading (digital cameras, whiteboards etc.)
- Any other internet enabled device.

Right to Online Access

We cannot stop advances in technology and nor should we try to do so. We should not prevent any member of our learning community from having access to such enabling resources. It should be recognised that children and young people have rights as learners. They should be entitled to have access to the most appropriate technologies to support their learning and development to prepare them for the 'real' world.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities (these lists are not intended to be exhaustive)

The Board of Trustees

- Trustees have overall responsibility for monitoring this policy and holding principals to account for its implementation. The Trustee who oversees online safety is our Safeguarding Trustee.
- The Head of Safeguarding will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL). The Head of Safeguarding will collate and share 360 Online Safety reports prepared by each academy with The Safeguarding Trustee.
- All Trustees will ensure that they have read and understand this policy, agree and adhere to the terms on acceptable use of the Trust IT systems and the internet (appendix 5), ensure that online safety is a running and interrelated theme while devising and implementing a whole Trust/Academy approach to safeguarding and related policies and/or procedures and ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

Executive Principals/ Principals/ Heads of Academy

The Executive Principal/ Principal/ Head of Academy is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

The Designated Safeguarding Lead

Details of the academy's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in each academy, in particular:

- Supporting the Executive Principal/ Principal/ Head of Academy in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy, as well as managing, logging, dealing with and addressing online safety issues or incidents in line with the Trust Child Protection and Safeguarding Policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour, anti-bullying and safeguarding policies
- Monitoring the filtering system of violation reports to ensure children are safe and supported to know how to keep safe on line.

- Updating and delivering staff training on online safety (appendix 6 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary and providing regular information on online safety in the academy to the Head of Safeguarding, who shares this within a termly report for Trustees.
- Providing reports about online safety in the Academy to the Head of Safeguarding and /or Board of Trustees

Head of IT and IT infrastructure manager

The IT manager/IT infrastructure manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material,
- Ensuring that the Trust/Academy's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly as well as conducting a full security check and monitoring the Trust/ Academy's IT systems on a regular basis,
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files. Managing systems to ensure any online safety incidents are logged and dealt with appropriately in line with this policy.

Academy Online Safety Group

- Each academy will appoint (an) individual(s) to oversee the use of online devices within the Academy. This is normally led by the HTTP for the Academy (Academy Lead on Computing) and may include HTML Advocates (Academy based Champions of using technology in the classroom). This group will monitor online safety within the academy, attend appropriate training, submit an annual review using the '360 Online Safety' document to the Head of Safeguarding, develop and implement an Online Safety Action Plan, respond to Academy specific incidents/trends within the Academy. The Group will include the views of pupils wherever possible (e.g., Student Council, Digital Leaders etc.) including their views on this policy.

All staff and volunteers, including agency staff, contractors, students, and volunteers.

- All staff, including contractors and agency staff, student and volunteers are responsible for maintaining an understanding of this policy, implementing it consistently, agreeing and adhering to the terms on acceptable use of the Trust/ Academy's IT systems and the internet (appendix 5), and ensuring that pupils follow the academy's terms on acceptable use (appendices 1 and 2).
- All adults will report online safety incidents, including those of cyber-bullying to the (D)DSL, and deal with these appropriately in line with the relevant policy. Staff will respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents/ Carers

- Parents/ carers are expected to notify a member of staff or the Executive Principal/ Principal/ Head of Academy of any concerns or queries regarding this policy, sign and adhere to the Acceptable Use Agreement and IT use Terms and Conditions for use of electronic equipment belonging to The Harmony Trust, ensure their child has read, understood, and agreed to the terms on acceptable use of the Trust's ICT systems and internet (appendices 1 and 2).

A list of sources of information for parents can be found here: [Sources of internet safety advice for parents](#)

Visitors and members of the community

- Visitors and members of the community who use the Academy's systems or internet will be made aware of this policy and If appropriate, they will be expected to agree to the terms on acceptable use (appendix 5).

4. Educating pupils about online safety

- Pupils will be taught about online safety as part of the curriculum, in accordance with the National Curriculum. The Trust's approach to the curriculum can be found here: [Educating pupils about online safety](#)
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

- The Academy will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via websites. This policy will also be shared with parents via the Academy's website.
- Parents and carers are made aware through the 'Acceptable Use Agreement' that the academy use a robust filtering and monitoring system to keep children safe online.
- Online safety information and workshops are provided for parents and carers to keep them up to date with advice and potential risks to protect their children from.
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Principal/ Principal/ Head of Academy and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Executive Principal/ Principal/ Head of Academy. Parents can access information through the [National Online Safety](#) website.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).
- Parents/ carers are also expected to sign an IT acceptable use agreement and support their child with this too.

6. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the academy's behaviour and anti-bullying policies).

Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The academy will actively discuss cyber-bullying with pupils at appropriate ages, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, trustees, volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
- The academy also sends information/leaflets on cyber-bullying to parents/ carers so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy behaviour and anti-bullying policies. Where illegal, inappropriate, or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The Executive Principal/ Principal/ Head of Academy, and any member of staff authorised to do so by SLT can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or,
- Is identified in the Academy rules as a banned item for which a search can be carried out, and/or,
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Executive Principal or Principal, explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it, and seek the pupil's co-operation,

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to cause harm, and/or, undermine the safe environment of the Academy or disrupt teaching, and/or, commit an offence.

If inappropriate material is found on the device, the staff member **MUST** report this to the DSL / Executive Principal/ Principal immediately so that a decision on a suitable response can be made in a timely manner. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be stored securely within the academy and handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or,
- The pupil and/or the parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with the DfE's latest guidance on [searching, screening and confiscation](#), UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#) and Academy behaviour policy and the Child Protection and Safeguarding Policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the academy complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools may have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. The Harmony Trust will treat any use of AI to bully pupils in line with our behaviour policy. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Harmony Trust.

7. Acceptable use of the internet in the Academy/ Trust

All users of Trust systems are expected to sign an agreement regarding the acceptable use of the Trust's/ academy's IT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant. Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, Trustees, and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendices 1 to 3.

7.1 Group specific use of the internet within Harmony Trust Establishments:

Staff:

Staff should only use Harmony Trust accounts when on a device connected to displays visible to the children – for example, and not limited to:

- personal accounts on sites such as Spotify, YouTube, Vimeo etc. Wherever possible, a separate account should be set up using a school email address.

Care must be taken when using streaming sites to limit children's exposure to advertisements, especially those which are not age appropriate. For example, when using YouTube, videos should be cued to the beginning of the video once advertisements have finished, or a suitable method of avoiding advertisements used.

Photographs should only be taken for legitimate Academy business. Where a photograph is taken, an Academy device such as a teachers' iPad or a Trust camera should be used. No other personal mobile device should be used in the presence of the children.

Early Years Foundation Stage Pupils:

Early Years settings require additional online safety measures that may be different to the rest of the school, due to the way the children access technology. The Trust provides additional guidance for Early Years classes in our academies. The guidance can be accessed here: [Additional Guidance for safe online use of technology in Early Years classes](#)

Key Stage 1 and 2 Pupils

Staff will build on the work in the previous Key Stage. All children will receive induction on how to use devices correctly according to their Key Stage, and then the academy will deliver IT lessons, PSHE lessons on Internet Safety as well as lessons in how to use devices across the curriculum. More specific information can be found in the guidance for Key Stages 1 and 2: [Additional Guidance for use of internet-linked devices in Key Stage 1 and 2](#)

Other children visiting an Academy

Non-Harmony Trust visiting children (such as siblings not at the Academy, visiting during Parents' Evenings or school performances) would not normally be expected to use the Internet whilst on Academy premises however they, may do so at the direction of a Trust employee for activities such as (but not limited to) translating for a parent/completing form for a parent/sibling). In such circumstances, Internet use should be closely supervised by a member of Trust staff and only for Trust/Academy business.

Professionals

Professionals may use the Academy Guest Wi-Fi system, provided that a copy of the Acceptable Use Agreement is signed. This can be found in appendix 3 and is also available as a Microsoft Forms document: <https://forms.office.com/e/hecG0ZSukC>. Guest access is only available whilst on Academy related business and is only available at the discretion of the Executive Principal/Headteacher/Head of Academy or DSL.

Parents

Parents should not be routinely given access to Trust IT systems (including Wi-Fi). Senior Leaders may decide to grant temporary access to systems to facilitate Trust requirements or to perform Trust business, but parents are normally expected to access the internet on their own internet enabled device. If such access to Trust systems is granted, parents must be closely supervised by a member of Trust staff.

All Users

All online communication must be polite, respectful, and non-abusive in manner. The Trust encourages emoticons to be used appropriately. Communication between adults and between adults and children should take place within the boundaries set out in this policy and for the purposes of education, as agreed in normal working practices and set out in each Acceptable Use Agreement.

8. Pupils using mobile devices in school

If pupils bring mobile devices into school, they must hand them into relevant staff for safe keeping until the end of the day (including after after-school clubs were applicable). See also Academy behaviour Policy.

In exceptional circumstances (such as a medical need), pupils may be permitted to use their own devices. A risk assessment and/or separate Acceptable Use Agreement should be drawn up by the Head of Academy and signed by all parties.

9. Pupils using Trust devices outside of school

Children are expected to use Trust devices allocated to them with the same level of safety and respect as they would within school. 1:1 iPads remain monitored outside of Academy premises and hours. Outside of school, parents take shared responsibility for monitoring their child's internet usage on a Trust device in line with the Acceptable Use Agreements (appendices 2 and 3) and the Terms and Conditions of Use (Appendix 2)

10. Staff using work devices outside school

The Trust IT Team ensures that all work devices have anti-virus and anti-spyware software installed, have operating systems that are kept up-to-date by always installing the latest updates and have encrypted hard drives – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to keeping the device password-protected with a strong password, locking devices when not attended and not sharing the device among family or friends. Work devices can be used for personal matters as long as the following conditions are met:

- Security is not compromised
- Is only used by the member of staff (not by family members or others)
- The content being looked at does not contravene any of our policies.
- The content is appropriate for children. Please be mindful of accessing any websites where there may be inadvertent links to inappropriate contact (e.g. social media sites)

Any content might be subject to scrutiny from any monitoring so staff must be aware of this when choosing to use a work device for personal matters. Concerns should be raised with line managers.

11. How the Trust/ Academy will respond to issues of misuse

Where a pupil misuses the Academy's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT and internet acceptable use agreements. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the Trust/ Academy's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/ staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The Trust/ Academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive induction training on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins, and staff meetings). Additional information can be found in the Academy's online safety policy.

13. Filtering and Monitoring arrangements

Filtering is provided by an external provider, dependent on the Academy. Monitoring is provided on pupil's 1:1 iPads through a third party system. This is then monitored by a team of staff in each academy. All staff have a responsibility to report any material that needs blocking, and this is normally raised to the (D)DSL. More information can be found in the guidance, here: [Additional Guidance on the use of Senso](#)

14. Protecting Personal Data

All staff should ensure that they do everything practicable to secure IT systems and ensure that personal data is protected. This includes ensuring password security, logging in and out, locating devices appropriately, restricting access to systems and using secure email address provided by the Trust. All devices are secured and wherever possible encrypted, and data should be transferred securely. Further guidance on how this can be achieved can be found in the guidance here: [Additional Guidance on Protecting Personal Data](#)

15. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy	Anti-bullying Policy	IT acceptable use agreements
Behaviour policy	Staff disciplinary procedures	Social Media Policy
Relationships Education	Data protection policy and privacy notices	Staff Code of Conduct
PSHE and safeguarding curriculum	Complaints procedure	

15. Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people based on their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. This policy has been equality impact assessed and we believe it is in line with the Equality Act 2010 and it is fair, it does not prioritise or disadvantage any pupil and it helps to promote and encourage equality in our academies.

16. Data Protection Statement

The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy. All data will be handled in accordance with the Academy's Data Protection Policy.

Data Audit for This Policy					
What?	Probable Content	Why?	Who?	Where?	When?
Online Safety policy	Name, address, personal information related to any online safety issues	Required to be retained as part of safeguarding process	Principal / SLT, Trust central team, staff or other representative as required as part of the safeguarding process	Kept on file at academy (and Trust central where appropriate)	Held on file until child leaves school and then passed onto new school

As such, our assessment is that this policy:

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
	X (KS2)	

Appendix 1: EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers)
(EYFS practitioners can use this for age-appropriate display and discussion as they consider appropriate)

ACCEPTABLE USE OF THE HARMONY TRUST'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Academy name:	
Name of pupil:	
Class:	
<p>When I use the school's ICT systems (like computers) and get onto the internet in school I will:</p> <ul style="list-style-type: none"> • Ask a teacher or adult if I can do so before using them, • Only use websites that a teacher or adult has told me or allowed me to use, • Tell my teacher immediately if: <ul style="list-style-type: none"> ○ I select a website by mistake, ○ I receive messages from people I don't know, ○ I find anything that may upset or harm me or my friends, • Use school computers for schoolwork only, • Be kind to others and not upset or be rude to them, • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly, • Only use the username and password I have been given, • Try my hardest to remember my username and password, • Never share my password with anyone, including my friends, • Never give my personal information (my name, address, or telephone numbers) to anyone without the permission of my teacher or parent/carer, • Save my work on the school network, • Check with my teacher before I print anything, • Lock, log off or shut down a computer when I have finished using it. <p>I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.</p>	
Signed (pupil):	Date:
<p>Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.</p>	
Signed (parent/carer):	Date:
<p>January 2024</p>	

Appendix 2: KS2 acceptable use agreement (pupils)



Acceptable Use Agreement (AUA) PUPILS



These statements can keep me and others safe & happy at school and home

To stay **SAFE** online and on my school device:

1. I only use devices or apps, sites or games with permission from a trusted adult. I know that my online activity is monitored.
2. I am secure online - I keep my passwords to myself and reset them if anyone finds them out. I do not give my details or address to anyone. S.M.A.R.T.



3. I will respect computing equipment and will immediately tell an adult if I notice something isn't working correctly or is damaged.
4. I look out for my friends and tell someone if they need help.
5. I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.
6. I know personal information such as my name, address and birthday should never be shared online.
7. I will always use my own username and password to access the school network and subscription services such as Purple Mash.
8. In order to help keep myself and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
9. Before I share, post or reply to anything online, I will T.H.I.N.K.



10. I understand that if I behave negatively whilst using technology towards other members of the school, my parents/ carers will be informed and appropriate actions taken.

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult.

At school that includes _____

Outside school, my trusted adults are _____

Signed: _____

Date: _____

I attended my induction training session on _____ **(Date)**

This AUA will remain in place throughout your child's career at the Academy. Your child will be reminded of this agreement regularly in order to keep them safe. If this AUA is updated, you and your child will be made fully aware of this. April 2021

Appendix 3: KS2 acceptable use agreement (parents/carers)



PARENT/ CARER - IT ACCEPTABLE USE AGREEMENT



These statements can keep my child and others safe & happy at school and home.

I will help my child to stay **SAFE** online and on their school device:

1. I will encourage my child to use devices or apps, sites or games that are age appropriate. I will monitor their online activity and discuss with them how to stay safe.
2. I will encourage my child to stay secure online – keep their passwords to themselves and reset them if anyone finds them out. I will ensure that they are reminded not to share details or address with anyone. S.M.A.R.T.
3. I will encourage my child to respect computing equipment and will tell the academy if I notice that something isn't working correctly or is damaged.
4. I will ensure that my child communicates and collaborates online – with people I already know and have met in real life or that I know about.
5. I will encourage my child to not share personal information such as their name, address, and birthday.
6. I will contact the academy if I have any concerns about my child's safety on-line. I will refrain from posting any concerns on social media sites and will contact the academy if I do have any issues or concerns, so that they can be resolved directly.
7. I will encourage my child not to share, post or reply to anything online that might endanger their safety or well-being.
8. I know that if my child behaves negatively whilst using technology towards other members of the school, I will be informed as their parent/ carer and appropriate actions will be taken.



- I have read, understood, and agree to these statements set out above.
- I agree that my child can use the Academy's IT systems/hardware & internet when appropriately supervised, including their own loaned i pad where this is applicable (from Y3 onwards)
- I know that my child is made aware of these statements regularly at school.
- I have signed up to the National Online Safety for guidance and free courses to support my child to be safe online.



Scan the QR Code to sign up for FREE at the National Online Safety website for guidance and free courses for parents.

Signed: _____

Parent/Carer of: _____

Class: _____

Date: _____

Appendix 4 : KS2 Terms and Conditions for use of Electronic Equipment (parents/carers)



Terms and conditions for use of electronic equipment belonging to The Harmony Trust

Dear Parent / Carer,

This document has been given so that you understand how the device that you have on loan from The Harmony Trust should be used and looked after while in your possession. It is intended that the main use of this device is so that your child can access the learning set through the academy via Purple Mash / School Spider. Your child may also use the device to view educational content such as BBC Bitesize.

Once loaned the device is the responsibility of the parent / carer and they should ensure that it is used in an appropriate way. The following are the terms which should be followed:

- The device remains the property of the Academy. The Academy may request the return of the device at any time, as such this device must not be sold or used as collateral.
- Upon signing for the device, charger and case become the responsibility of the signatory until it is returned to the Academy,
- The signatory agrees to responsible usage of the device. Parents should provide appropriate supervision to their child when using the device (Additional materials are provided to support parents.) This device should only be used by the pupil it is allocated to, for educational support purposes,
- Any misuse, inappropriate material or un-copyrighted software held on the device is their responsibility,
- Files and media should not be saved to the device; this will be wiped permanently upon return. Children must save their work on 'OneDrive' and will be taught how to do this in school,
- If a problem is encountered. It should be reported to the academy as soon as possible. There should be no attempt to disassemble any parts as this could invalidate the warranty,
- Adequate precautions should be taken to protect from theft, misuse, or damage of the device.
- Connection to the Internet and its cost remain the responsibility of the signatory. The academy and / or Trust will accept no costs,
- Adequate precautions should be taken to ensure no computer virus or other malicious program is downloaded to the device. Any damage to a home network caused by viruses or malfunctions of the device is not the liability of the Trust,
- The Trust will be recording all IP addresses from different Wi-Fi systems that the device has been joined to. GPS/location tracking is also enabled on the device and as such this information is recorded by the system.

By signing this document, you agree to abide by the terms and conditions and acknowledge that you are aware that your child has signed an acceptable use agreement in the Academy and the points within this agreement.

Parents and Carers should be aware that The Harmony Trust has installed Internet monitoring software on the device. This means that we are able to filter and monitor internet use and the website content that is being accessed.


Signed _____

Print Name _____ Date _____

For Academy Use – Name of Device _____

Appendix 5: Acceptable Use Agreement (Staff, Trustees, Volunteers, Students and Visitors)

This is also available as a Microsoft Forms document: <https://forms.office.com/e/hecG0ZSukC>

 THE HARMONY TRUST <small>BELIEVE • ACHIEVE • SUCCEED</small>	
ACCEPTABLE USE OF THE TRUST/ ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS. STUDENTS AND VISITORS	
Name of Staff member/ Trustee/Volunteer/Student / Visitor	
Representing:	
<p>When using the Academy's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:</p> <ul style="list-style-type: none"> • Access, or attempt to access inappropriate material, including but not limited to material of a violent, <u>criminal</u> or pornographic nature (or create, share, link to or send such material), • Use them in any way which could harm the Trust/ Academy's reputation, • Access social networking sites or chat rooms, • Use any improper language when communicating online, including in emails or other messaging services, • Install any unauthorised software, or connect unauthorised hardware or devices to the Trust/ Academy's network, • Share my password with others or log in to the Trust/ Academy's network using someone else's details, • Take photographs of pupils without checking with Teachers and Senior Leaders first, • Share confidential information about the Trust/ Academy, its pupils or staff, or other members of the community, • Access, modify or share data I'm not authorised to access, modify or share, • Promote private businesses unless that business is directly related to the Trust/ Academy. 	
<p>I will only use the Trust/ Academy's ICT systems and access the internet in an Academy, or outside an Academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the Trust/ Academy will monitor the websites I visit and my use of the Trust's/ Academy's ICT facilities and systems.</p> <p>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Trust/ Academy, and keep all data securely stored in accordance with this policy and the Trusts' data protection policy.</p> <p>I will let the designated safeguarding lead (DSL), Principal, Head of Academy or my line manager and the ICT manager know if a pupil informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.</p> <p>I will always use the Trust's/ Academy's ICT systems and internet responsibly and ensure that pupils in my care do so too.</p>	
Signed (Staff member/ Trustee/ Volunteer/ Student/ Visitor):	
Date:	
<small>A signed copy should be retained by the Academy – January 2024</small>	

Appendix 6: Online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Comment
What is the name of the person who has lead responsibility for online safety in our academy?	
List the ways pupils can abuse their peers online?	
What must you do if a pupil approaches you with a concern or issue?	
Are you familiar with the academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the academy's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the academy's ICT systems?	
Are you familiar with the academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 7: Senso Security Data Sheet

REVISED: JANUARY 7TH, 2018

Data in transit

Senso.cloud uses industry-standard protocols to encrypt data in transit as it travels between devices and Microsoft datacenters, which are used to host the senso servers. When data moves within Microsoft datacenters and data is at rest within Azure Storage, security capabilities include:

- Protection for data in transit and at rest, including encryption for data, files, applications, services, communications, and drives.
- Support for and use of numerous encryption mechanisms, including SSL/TLS, IPsec, and AES.
- Access to stored data by Microsoft Azure support personnel requires senso.cloud explicit permission and is granted on a “just in time” basis that is logged and audited, then revoked after completion of the engagement.

Senso Security

Security along with user control is built right into the senso.cloud platform, beginning with TLS encrypted data communication to applying console access rights to individual console users.

- All senso.cloud databases are IP restricted to our physical offices.
- Backend senso.cloud Azure configuration/tenancy is protected by two-factor authentication.
- All data access is time limited for authorised users only and restricted to the lowest possible level of access.
- Auditing has been enabled on all senso databases.
- Microsoft Threat Detection enabled on all senso databases.
- There are no senso staff “master” accounts; in the unlikely event that one of our staff accounts was compromised, this cannot be used to access any customer accounts.
- All senso modules are hashed and only modules that have the correct hash are allowed to run.
- Access to your portal by senso support personnel requires your explicit permission and is granted by you on a “just in time” basis that is logged and audited in your console, then revoked by you after completion of the engagement.
- Access to your data is read only and cannot be tampered with by users at your organization.
- All devices need approval before they are shown in the senso portal.

Shared responsibilities

Customers must implement security best practices and educate users on how to access cloud services securely just as you would with email services. To improve our security offering we have integrated with Microsoft and Google accounts which offer their own two factor authentication methods. In addition, we are planning to add login hour restrictions and public IP lockdown to the console.

Appendix 8: Online Safety Policy Review and Audit - Academies to Complete



Online Safety Policy Checklist

		Yes	No	Don't know
1	Do you have an Online Safety Policy			
2	Are policies / practice reviewed regularly (annually)?			
3	Are policies linked and coordinated - e.g., Online Safety / Behaviour / Curriculum / Anti-Bullying / Staff Discipline etc			
4	Does regular monitoring / review of online behaviours and / incidents impact on the policy review?			
5	Do you have an AUP for:			
	Students / Pupils / Members			
	Staff / Volunteers			
	Other users			
6	Do you have a Designated Person responsible for online safety e.g., an Online Safety Lead			
7	Would your online safety provision suffer significantly if this person left?			
8	Do you have an Online Safety Group?			
9	Does the Online Safety Committee have wide representation?			
10	Does this include students/pupils/young people (Council etc)?			
11	Are staff & volunteers adequately trained?			
	At induction?			
	Regular updates			
	All staff (not just teachers in academies!)?			
	Safeguarding / Online Safety training linked?			
12	Do young people receive good online safety education?			
	For all students / pupils / members?			
	Is it planned / mapped?			
	Is it regularly revisited?			
	Is it age appropriate?			
	Is it across the curriculum, not just in ICT / Computing?			
13				

	Are there clear and well-known procedures for online safety incidents to be reported?			
	Is there effective filtering and monitoring in place?			
	Is the filtering provided by an accredited supplier?			
	Is the filtering differentiated by age?			
	Is the filtering flexible? (Does it support educational objectives)			
	Are those responsible for the administration of the filtering adequately supervised / supported by senior leaders?			
	Is the filtering supported by monitoring systems?			
14	Are online safety incidents logged?			
15	Do policies help staff and volunteers understand the need to protect their online reputation?			
16	Do policies make it clear to staff and volunteers how they should (or should not) communicate electronically with students / pupils / young people / parents and carers?			
17	Are policies clear in establishing which online technologies can be used by staff / volunteers and by pupils / students / young people and when / how they can be used?			
18	Do policies make it clear that online safety incidents outside the academy are covered by the policy if they impact on the academy?			
19	Do the policies make it clear what items may be searched for, how and by whom? (n.b. Education Act 2011)			
20	Do policies make it clear what and how can be deleted from electronic devices (n.b. Education Act 2011)			
21	Other organisations (not covered by the Education Acts) - do you have clear procedures for search / deletion (as in 19 / 20 above)			
22	Is Personal Data held by the organisation well protected by policies and procedures?			
	Are there clear policies about protecting personal data?			
	Are all staff and volunteers aware of these policies?			
	Are rules clear re transferring data/laptop security/memory sticks etc?			
	Is encryption used for all data taken / transferred off site?			
23	Are there clear sanctions in place for the misuse of online technologies and are these clearly understood by users?			
24	Is there a clearly understood policy for the use of digital images and video?			
25	Were you confident, when answering these questions that:			
	You knew the answers?			
	Others (preferably all) in your academy would know?			
	Online Safety is embedded in your academy organisation?			