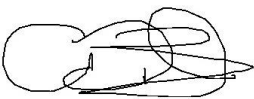



Online safety policy 2023

Signed (chair): 	Name: Andrew Bowden	Date: 16/11/2023
Signed (Head): 	Name: Tracy French	Date: 16/11/2023
Ratified by: Trust Board on: 16/11/2023		Next Review: November 2024
<p>Policy Updates</p> <p>May 2022 Each new academic year staff sign an annual declaration stating, 'I can confirm that I have read, understood and agree to abide by the guidelines set out the ICT, e-mail and internet acceptable use policies.'</p> <p>October 2023 Policy upgrade to current version as detailed in KCSIE 2023 Policy has been renamed – Previously E-Safety policy. Now - Online safety policy. This new policy also incorporates the previous ICT, email and acceptable use policy.</p>		

Contents

1. Legislation and guidance	2
2. Roles and responsibilities	3
3. Educating pupils about online safety	5
4. Educating parents/carers about online safety	6
5. Cyber-bullying	6
6. Acceptable use of the internet in Academy	8
7. Staff using work devices outside Academy	8
8. How the Academy will respond to issues of misuse.....	8
9. Training	9
10. Monitoring arrangements.....	9
11. Links with other policies.....	9
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers).....	10
Appendix 2: KS2, acceptable use agreement (pupils and parents/carers)	11
Appendix 3: acceptable use agreement (Staff, Trustees, Local Academy Councillors, Volunteers and Visitors)	12
Appendix 4: online safety training needs – self-audit for staff	13

Aims

Waycroft Multi Academy Trust aims to:

- › Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Trustees and Local Academy Councillors
- › Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- › 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

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

1. 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 Academics on:

- › [Teaching online safety in Academics](#)
- › [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and Academy 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 inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

2. Roles and responsibilities

2.1 The Trust Board and Local Academy Councils

The Trust board has overall responsibility for monitoring this policy and holding the Executive Headteacher and Headteachers to account for its implementation.

The Local Academy Councils for each academy will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Local Academy Council will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Trust Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Trust board must ensure the Academy has appropriate filtering and monitoring systems in place on academy devices and networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with the Executive Headteacher, IT staff and service providers what needs to be done to support the Academy in meeting standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

All Trustees, Local Academy Councillors will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the MAT's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-Trust approach to safeguarding and related policies and/or procedures.
- 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.

2.2 The headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

- › Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- › Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy behaviour policy.

2.3 The designated safeguarding lead

Details of the Academy's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in each of our academies, in particular:

- › Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy.
- › Working with the Headteacher and Local Academy Council to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- › Working with the ICT technician to make sure the appropriate systems and processes are in place.
- › Working with the Headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents.
- › Managing all online safety issues and incidents in line with the Academy's child protection policy
- › Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- › Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy.
- › Liaising with other agencies and/or external services if necessary.
- › Undertaking annual risk assessments that consider and reflect the risks children face.
- › Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

2.4 The ICT technician

The ICT technician is responsible for:

- › Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on Academy devices and Academy networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at Academy, including terrorist and extremist material.
- › Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- › Taking the lead on understanding the filtering and monitoring systems and processes in place on Academy devices and Academy networks.
- › Windows defender and Bristol City Council Netsweeper constantly monitor the IT system, the IT technician will receive an alert should there be a potential breach. All user accounts are password protected.
- › Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- › Providing regular reports on online safety in Academy to the Executive Headteacher.

This list is not intended to be exhaustive.

2.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- › Maintaining an understanding of this policy
- › Implementing this policy consistently
- › Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 3), and ensuring that pupils follow the Academy's terms on acceptable use (appendices 1 and 2)
- › Knowing that the IT Technician is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by reporting on CPOMS, or informing a DSL.
- › Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- › Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy.
- › Responding 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.

2.6 Parents/carers

Parents/carers are expected to:

- › Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- › Ensure their child has read, understood and agreed to the terms on acceptable use of the Academy's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- › What are the issues? – [UK Safer Internet Centre](#)
- › Hot topics – [Childnet International](#)
- › Parent resource sheet – [Childnet International](#)

2.7 Visitors and members of the community

Visitors and members of the community who use the Academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

3. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All Academies have to teach:

- › [Relationships education and health education](#) in primary Academies

In **Key Stage (KS) 1**, pupils will be taught to:

- › Use technology safely and respectfully, keeping personal information private.
- › Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage (KS) 2** will be taught to:

- › Use technology safely, respectfully, and responsibly.
- › Recognise acceptable and unacceptable behaviour.
- › Identify a range of ways to report concerns about content and contact.

By the **end of primary Academy**, pupils will know:

- › That people sometimes behave differently online, including by pretending to be someone they are not.

- › That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
- › The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- › How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- › How information and data is shared and used online
- › What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- › How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4. Educating parents/carers about online safety

The Academy will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our websites. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The Academy will let parents/carers know:

- › What systems the Academy uses to filter and monitor online use
- › What their children are being asked to do online, including the sites they will be asked to access and who from the Academy (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

5. Cyber-bullying

5.1 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.

5.2 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, 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.

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour policy. 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.

5.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher 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 the Headteacher / DSL / appropriate staff member.
- › Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- › 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, it is up to the staff member in conjunction with the DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. 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 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/carer 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](#)

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

5.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Waycroft Multi Academy Trust recognises that AI has many uses to help pupils learn but may also 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.

Waycroft Multi Academy Trust will treat any use of AI to bully pupils in line with our anti-bullying/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 Academy/trust.

6. Acceptable use of the internet in Academy

All pupils, parents/carers, staff, volunteers and Trustees and Local Academy Councillors are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the Trust'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, Local Academy Councillors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

7. Staff using work devices outside Academy

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
- › Ensuring their hard drive is encrypted – 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
- › Making sure the device locks if left inactive for a period of time
- › Not sharing the device among family or friends
- › Ensuring anti-virus and anti-spyware software is installed
- › Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the Academy's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

8. How the Academy will respond to issues of misuse

Where a pupil misuses the Academy's ICT systems or internet, we will follow the procedures set out in our behaviour policy - 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 Academy's ICT 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 academy will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Training

All new staff members will receive training, as part of their induction, 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 and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
 - Abusive, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees, Local Academy Councillors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

10. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every year by the Executive Headteacher at every review, the policy will be shared with the Trust board.

11. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the Academy's ICT systems (like computers) and get onto the internet in school I will:

- 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:
 - 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 Academy computers for Academy work only;
- Be kind to others and not upset or be rude to them;
- Look after the Academy 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 Academy network;
- Check with my teacher before I print anything;
- Log off or shut down a computer when I have finished using it.

I agree that the Academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of Academy staff. I agree to the conditions set out above for pupils using the Academy's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: KS2, acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the Academy's ICT systems (like computers) and get onto the internet in school I will:

- Always use the Academy's ICT systems and the internet responsibly and for educational purposes only;
- Only use them when a teacher is present, or with a teacher's permission;
- Keep my usernames and passwords safe and not share these with others;
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer;
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others;
- Always log off or shut down a computer when I've finished working on it.

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity;
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher;
- Use any inappropriate language when communicating online, including in emails;
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate;
- Log in to the Academy's network using someone else's details;
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision;

If I bring a personal mobile phone or other personal electronic device into Academy:

- I will hand it in on arrival to collect at the end of the day.

I agree that the Academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of Academy staff. I agree to the conditions set out above for pupils using the Academy's ICT systems and internet, and for using personal electronic devices in the Academy, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 3: acceptable use agreement (Staff, Trustees, Local Academy Councillors, Volunteers and Visitors)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, LOCAL ACADEMY COUNCILLORS, VOLUNTEERS AND VISITORS

Name:

When using the Trust's ICT systems and accessing the internet within in, or outside Waycroft MAT on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the Academy/Trust's reputation;
- Access social networking sites or chat rooms for my own personal use;
- 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 Academy's network;
- Share my password with others or log in to the Academy's network using someone else's details;
- Take photographs of pupils without checking with teachers first;
- Share confidential information about the 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 Academy/Trust;
- Attempt to bypass security in place on the computers, or attempt to alter the settings;

In addition:

- If any work device is stolen, it must be reported to the DPO immediately as this is considered a breach under GDPR and will need reporting within 72 hours;
- I understand I am responsible for the repair and maintenance costs of laptops (hardware and software) necessary due to negligence or misuse;
- Where applicable, I will ensure appropriate and safe care and storage of school laptops when at home and when travelling;
- If employed in the capacity of a teacher/HLTA, I understand I have a responsibility to monitor the range of sites used and should pre-plan sites to be accessed with the children during lessons.

I will only use the Academy's ICT systems and access the internet in Waycroft MAT, or outside Waycroft MAT on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the Trust will monitor the websites I visit and my use of the Trust's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside of the Academy, and keep all data securely stored in accordance with this policy and the MAT's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT technician 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.

I will always use the Academy's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed:

Date:

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in this Academy?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the Academy's acceptable use agreement for staff, volunteers, Trustees, Local Academy Councillors and visitors?	
Are you familiar with the Academy's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the Academy's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	