Upwell Academy

Online Safety Policy

September 2025

Policy owner	Academy Committee
Author	Chris Harris, Principal

Approved by

Consultation Group	Senior Leadership Team
Approval Committee	Academy Committee
Implementation Date	September 2025
Review Date	September 2028

Version Control

Version	Summary of Changes	Consultation Group	Effective Date
1.0	New Policy - no changes	Senior Leadership Team	September 2025

Contents

1. Aims

Our academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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 (including mobile phones)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2 The four 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, anti-Semitism, 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 scam

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: advice for Principals 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 cyberbullying 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 takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Academy Committee

The academy committee has overall responsibility for monitoring this policy and holding the principal to account for its implementation.

The academy committee 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 academy committee will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The academy committee 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) team.

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

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

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-academy 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

3.2 The Principal

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

3.3 The Designated Safeguarding Lead (DSL) Team

Details of the academy's DSL team are set out in our safeguarding policy as well as relevant job descriptions.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the Principal and academy committee to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on academy devices and academy networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the IT Support (TIO) to make sure the appropriate systems and processes are in place
- Working with the Executive Principal, IT Support (TIO) 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

- Responding to safeguarding concerns identified by filtering and monitoring
- 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 and anti-bullying policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in academy to the principal and/or academy committee
- 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, to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 IT support (TIO)

IT support is provided by Turn It On (TIO) and 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 the 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
- Conducting a full security check and monitoring the academy's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 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 DSL team 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 alerting the DSL team for an immediate response

- Following the correct procedures by getting authorisation from the principal and then contacting IT Support (TIO) if they need to bypass the filtering and monitoring systems for educational purposes

- Working with the safeguarding team 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.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the principal 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 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

- Healthy relationships – Disrespect Nobody

3.7 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).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum using the guidance on relationships education, relationships and sex education (RSE) and health education.

In **Key Stage 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
- Use the SMART on-line safety rules (Stay **S**afe, don't **M**eet up, don't **A**ccept files or requests, how **R**eliable is the information, **T**ell an adult) www.kidsmart.org.uk (See Appendix 4)

Pupils in **Key Stage 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
- Use the SMART on-line safety rules (Stay **S**afe, don't **M**eet up, don't **A**ccept files or requests, how **R**eliable is the information, **T**ell an adult) www.kidsmart.org.uk (See Appendix 4)

By the **end of primary school**, 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.

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

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

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

If a child shares that they have watched or accessed age-inappropriate technology, video, television, social media, etc., their parent/carer will be contacted to discuss ways to keep their child safe.

6. Cyberbullying

6.1 Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is persistently, deliberately hurtful or threatening and targeted behaviour. It is not a one-off isolated incident. See also the academy's behaviour policy and anti-bullying policy.

6.2 Preventing and Addressing Cyberbullying

To help prevent cyberbullying, 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 witnesses rather than victims.

The academy will actively discuss cyberbullying 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.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, 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 cyberbullying to parents 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 cyberbullying, the academy will follow the processes set out in the academy's 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 team will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

All online safety concerns are recorded on CPOMS and are regularly reviewed by the DSL team.

6.3 Examining Electronic Devices

The principal and any member of staff authorised to do so by the principal 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:

- Make an assessment of 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 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
- 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 principal 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 team immediately, who will decide what to do next. The DSL team will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Committee 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 / EMAT's complaints procedure.

6.4 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 Gemini.

We recognise 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils very seriously, in line with our behaviour and anti-bullying 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 the academy is using new AI tools and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

7. Acceptable use of the Internet in the academy

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (appendices 1-2). 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, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in the academy

Mobile devices include, but are not limited to, mobile phones, smart watches or any other digital device capable of recording and/or sending text, sound, images, data or video.

If a pupil has a mobile device agreement (appendix 5) signed by a parent/carer then they may bring mobile devices into the academy. Mobile devices must be switched off before coming on site.

At the start of the day, all pupils must turn off their mobile devices before coming on site. They must place their devices into a named bag and hand them to the adult in charge of their class. The mobile device will be stored in a lockable box and placed in a cupboard in the classroom. The mobile device will be returned to the pupils at the end of the academy day.

If a child has a mobile device switched on whilst on site, then this will be a breach of the mobile device agreement and could lead to the pupil being banned from having a mobile device on site.

Exceptions to the mobile device agreement, e.g. for medical reasons – such as blood sugar tracking, must be authorised in writing by the principal as part of a health care plan.

9. Staff using work devices outside of the 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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

IT support will also help by:

- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which 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 IT support.

10. 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 policies on behaviour and ICT and internet acceptable use. 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. 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, e-bulletins 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 the risks up
- 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 Team 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.

Governors 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.

12. Monitoring arrangements

CPOMS is used to log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL Team. At every review, the policy will be shared with the academy committee. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. 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
- ICT and internet acceptable use policy

Appendix 1: Acceptable use agreement for pupils and parents/carers

Name of pupil:	
When I use the academy's ICT facilities (like computers and equipment) and get on the internet in academy, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break academy rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes • Share my password with others or log in using someone else's name or password • Bully other people • Use AI tools without permission of my teacher I understand that the academy will check the websites I visit and how I use the academy's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on an academy computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the academy's ICT systems and internet. I understand that the academy can discipline me if I do certain unacceptable things online, even if I'm not in the academy when I do them.	
Signed (KS2 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 for using personal electronic devices in the academy, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Adult acceptable use agreement (staff, governors, volunteers and visitors)

To ensure that members of staff are fully aware of their professional responsibilities when using ICT systems and equipment, staff are required to sign this document. Members of staff must read and understand the Trust's IT Security Policy, E-Safety Policy and the Acceptable use of ICT Policy prior to signing.

Name of staff member/governor/volunteer/visitor:

I understand that the Trust's ICT equipment is the property of the Trust whether used on or off the premises.

I understand that the Trust's ICT systems and services must be used in accordance with Trust policies whether used on or off the premises.

I understand that it is a disciplinary offence to use any Trust ICT system, services or equipment for a purpose not permitted by the Trust. This includes (but is not limited to):

- conducting illegal activities
- accessing or downloading pornographic material
- political purposes
- gambling
- soliciting for personal gain or profit
- managing or providing a business service using the Internet
- advertising
- revealing or publicising proprietary or confidential information
- representing personal opinions as those of the Trust, or saying to speak on behalf of the Trust
- making or posting indecent remarks or proposals
- sending chain letters
- using software in violation of its copyright
- Illegal downloading from torrent sites (copyright music and films etc.)
- intentionally interfering with the normal operation of Trust Internet services, Learning Platform services, Management Information System, hardware or software

(Staff are permitted to browse the internet and undertake activities such as online shopping during non-contact time (teachers) or designated breaks (support staff)).

I understand that my use of Trust systems, software, Internet and email is monitored and recorded to ensure policy compliance. Where the Trust believes that unauthorised use of equipment, systems or services may be taking place, it may delete inappropriate materials and may take disciplinary action. Where the Trust believes that equipment, systems or services may be being used for unlawful or criminal purposes this may be referred to the appropriate agency.

I accept that I am responsible for the use and protection of the user credentials with which I am provided (user account and password, access token or other items I may be provided with)

I will not attempt to access any computer system to which I not been given access. I will respect system security, and I will not disclose or share any login, password or security information to anyone other than an authorised system manager. I will not use anyone else's user account and password to access company systems

I will protect any sensitive material sent, received, stored or processed by me according to the level of classification assigned to it, including both electronic and paper copies

I will not send classified or sensitive information over the Internet via email or other methods unless appropriate methods (e.g. encryption) have been used to protect it from unauthorised access

I will always ensure that I enter the correct recipient email address(es) so that sensitive information is not compromised

I will ensure I am not overlooked by unauthorised people when working and will take appropriate care when printing sensitive information

I will securely store sensitive printed material and ensure it is correctly destroyed when no longer needed

I will not leave my computer unattended such that unauthorised access can be gained to information via my account while I am away

I will make myself familiar with the organisation's security policies and procedures and any special instructions relating to my work

I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security

I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended

I will not remove equipment or information from the organisation's premises without appropriate approval

I will not introduce viruses or other malware into the system or network

I will not attempt to disable anti-virus protection provided at my computer

I will comply with the legal, statutory or contractual obligations that the organisation informs me are relevant to my role

On leaving the organisation, I will inform my manager prior to departure of any important information held in my account

I understand that ICT includes a wide range of systems, includes but not limited to mobile phones, digital cameras, email and social networking. ICT use may also include personal ICT devices with the permission of the principal if used for Trust business.

I understand that I must not communicate with current students of the Trust via public social networking sites (e.g. Facebook, Twitter, Instagram) and that if contact is required, I must use Trust-owned equipment or facilities (e.g. the email facility on the Learning Platform or MIS or a phone provided by the Trust).
I understand that my use of social networking sites (e.g. Facebook, Twitter, Instagram) should be for personal use only; however, should there be a requirement to use social media for Trust purposes then my usage will be consistent with my professional role. All communication with parents of students at the Trust should be conducted using Trust-owned equipment or facilities (e.g. the email facility on the Learning Platform, MIS or a phone provided by the Trust).

I understand that my use and storage of photographic images or video recordings of pupils taken in Trust or on Trust activities should be with parental/student consent.

I understand that any official Trust blogs, wikis, discussion boards etc. should be hosted on the Trust's website or Learning Platform, SharePoint/intranet.

I will respect and abide by all copyright and intellectual property rights.

I will ensure that all Trust electronic communications that I make are compatible with my professional role and Trust policies and will not use inappropriate humour, graphics or images.

I will seek to ensure that I check my email inbox each working day and deal with emails promptly and I will maintain my user area(s) in good order whether on a laptop or on networked computers or other devices.

I will ensure that students are appropriately supervised when using ICT equipment and remind them that their ICT activity is routinely monitored.

I will ensure that I will use AI tools ethically and in line with Academy or Trust policies, ensuring that AI use does not compromise academic integrity or safeguarding.

I will take all steps necessary for the protection of both IT and information whilst it is in my possession, and I will also ensure that I either log off my computer or apply the screen lock should I need to leave the computer for any reason.

I will ensure that personal data is stored securely and is used appropriately, whether in Trust, taken off the Trust premises or accessed remotely. I will ensure that personal or confidential information is not stored on any computers not belonging to the Trust or on removable media, such as memory sticks, CDs etc except for the purpose of transfer of data from one Trust's computer to another Trust's computer, using encryption. I will ensure that no personal data is copied unless there is a specific legitimate requirement to do so.

I understand that computers provided by the Trust for use away from the Trust premises may be used for personal purposes provided that any usage does not constitute a breach of this or any other Trust policy or Code of Conduct.

I will not install any software or hardware without authorisation by the rincipal or Trust's Chief Finance Officer
.

If using a computer provided by the Trust away from Trust premises, I will ensure that appropriate physical security measures are in place to safeguard the equipment. I will also ensure that any anti-virus protection software is updated prior to leaving the Trust. I will report any information breach and/or security incidents of concern relating to the inappropriate use of ICT systems or equipment to the Academy or Trust Data Lead, the Designated Child Protection coordinator or Principal. **I have read, understood and accept the obligations outlined above for Acceptable Use of ICT.**	
Signed (staff member/governor/volunteer/visitor):	**Date:**
Please sign and return to your Academy Principal or HR within one week of receipt	

Appendix 3: Online Safety Training

Online safety training needs – Self-Audit	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know who has lead responsibility for online safety in 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, 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 4: SMART Rules Poster

Appendix 5: Mobile Device Agreement

<table>
<tr><th colspan="2">MOBILE DEVICE agreement for pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">Mobile devices include, but are not limited to, mobile phones, smart watches or any other digital device capable of recording and/or sending text, sound, images, data or video.
I agree to do the following:

• I will turn off all mobile devices before coming on to the academy site.
• As soon as I am in class, I will place all my mobile devices into my named bag.
• I will hand my named bag to the adult in charge of my class.
My mobile devices will be stored in a lockable box and placed in a cupboard in the classroom.
At the end of the academy day, my mobile devices will be returned to me.
I will not turn on my mobile devices until I am off site.
I agree that the academy may check, at any time, that my mobile devices are switched off.
I understand that if I don’t follow this agreement then my mobile devices may be confiscated and held at the office for a parent/carer to collect.
I understand that, for any reason, the academy may withdraw permission for me to bring my mobile devices to the academy.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement:
I agree that my child may bring mobile devices to the academy.
I agree that the academy does not accept any responsibility for loss or damage to any mobile device.
I understand that should my child not follow the mobile device agreement, then the mobile device may be confiscated and held at the academy office for a parent/carer to collect.
The academy may withdraw permission for my child to bring mobile devices to the academy for any reason.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>