Batley Multi Academy Trust

Online Safety Policy

Batley Multi Academy Trust

Approved by: Board of Trustees	**Ratified:** September 2026
Last reviewed on: September 2026	**Next review due by:** September 2027
Reviewed by: Director of IT	

Aims

This Online Safety policy has been created by Batley Multi Academy Trust ('the Trust'), building on existing templates, with specialist advice and input as required.

The purpose of this policy is to:

- Safeguard and protect all members of the Trust community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.
- Have robust processes in place to ensure the online safety of our learners, colleagues and volunteers. For the purpose of this policy, the term volunteers covers all layers of governance (Members, Trustees and Governors) as well as those in volunteer roles at each school.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school 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 Trust identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, such as pornography, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example, 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; for example, making, sending, and receiving explicit images (including those generated or manipulated using artificial intelligence/deepfakes, as well as consensual and non-consensual sharing of nudes and semi-nudes) and online bullying
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If you have concerns about this, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Legislation and Guidance

This policy takes into account and is based on:

- Keeping children safe in education - GOV.UK
- Teaching online safety in schools - GOV.UK
- Early years foundation stage statutory framework (EYFS)
- Working together to safeguard children - GOV.UK
- Preventing bullying - GOV.UK
- Protecting children from radicalisation: the prevent duty
- Searching, screening and confiscation
- Cyberbullying: Advice for headteachers and school staff

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

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 young peoples' electronic devices where they believe there is a 'good reason' to do so.

Scope

- The Trust believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all stakeholders are protected from potential harm online.
- The Trust identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- The Trust believes that all young people should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy complies with our Funding Agreement and Articles of Association.

Monitoring and Review

- The Trust will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns, or any changes to the technical infrastructure.
- We will ensure that we regularly assess internet use, and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Trust Headteachers, CEO and Trustees will be informed of online safety concerns, as appropriate.
- The relevant sub committee at Trust level will monitor online safety concerns via the safeguarding report submitted by the Trust Safeguarding Lead.
- Any issues identified will be incorporated into the Trust's action planning.

Roles and Responsibilities

- The Board of Trustees has overall responsibility for monitoring this policy and holding Trust Headteachers to account for its implementation.
- Each school within the Trust has an appointed Designated Safeguarding Lead (DSL).
- Each school within the Trust may also have appointed an Online Safety Lead (OSL).
- The Trust recognises that all members of the community have important roles and responsibilities to play with regards to online safety.
- The CEO will ensure the Trust Central Team follows all online safety protocols and procedures.

The Senior Leadership Teams (SLT) in each school will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Along with the DSL, ensure that suitable and appropriate filtering and monitoring systems are in place (Appendix A).
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSLs and OSLs by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments and where necessary, Data Protection Impact Assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

This list is not intended to be exhaustive.

The DSLs will:

- Support SLT in ensuring that staff understand this policy and that it is being implemented consistently throughout their school.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Managing all online safety issues and incidents in line with the Safeguarding and Child Protection policy, ensuring that any online safety incidents are logged and responded to appropriately, in line with this policy.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

- Ensure that online safety is promoted to parents/carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the SLT, CEO and Trustees.
- Work with the SLT to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the Governor with a lead responsibility for safeguarding and/or online safety.

This list is not intended to be exhaustive.

The Trust's Director of IT

The Trust's Director of IT 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 learners are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the Trust'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 Trust's ICT systems on a routine basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with each school's relevant policy.

This list is not intended to be exhaustive.

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and SLT, and Trust team.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that each school's and the Trust's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that each school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the SLT.
- Report any filtering breaches to the DSL and SLT, as well as each school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring

or filtering breaches are reported to the DSL in accordance with the Trust's safeguarding procedures.
- Ensure the Trust's Director of IT is kept up to date and informed of any of the above incidents, where relevant.

All Staff

It is the responsibility of all staff, including volunteers, contractors and agency staff to:

- Contribute to the development of online safety policies.
- Maintaining an understanding of this policy.
- Implement this policy consistently.
- Read and adhere to the online safety policy and acceptable use policies (AUP).
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the young people in their care.
- Identify online safety concerns and take appropriate action by following the Trust's Safeguarding and Child Protection policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

Young People

It is the responsibility of all learners, (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the AUP.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

Parents/Carers

It is the responsibility of parents/carers to:

- Read the AUP and encourage learners to adhere to it.
- Support the Trust in their online safety approaches by discussing online safety issues and reinforcing appropriate, safe online behaviours both in and out of school, on all devices.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and Trust's AUP.
- Identify changes in behaviour that could indicate that a person is at risk of harm online.

- Seek help and support from the school, or other appropriate agencies, if they, or someone they know encounters risks or concerns online.
- Contribute to the development of the Trust's Online Safety policy.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- 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
    - CEOP - https://www.ceop.police.uk/Safety-Centre/

Visitors
Visitors who use the 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.

Educating Learners about Online Safety
Learners will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, learners 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.

Learners in **Key Stage 2,** learners 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 school**, learners 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.

In **Key Stage 3**, learners will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns, including cyber bullying and grooming.

In **Key Stage 4,** learners will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns e.g. cyber bullying, grooming.

By the **end of secondary school**, learners will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online. Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).
- 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 learners, victims of abuse and learners with SEND.

Education and Engagement Approaches

Education and engagement with learners

Each school will establish and embed a progressive online safety curriculum throughout, to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the PSHCE and Computing programmes of study, covering use both at school and at home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and show them how to validate information before accepting its accuracy.

The Trust will support learners to read and understand the AUPs in a way which suits their age and ability by:

- Informing users that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Using support, such as external visitors, where appropriate, to complement and support the Trust's internal online safety education approaches.

Vulnerable learners

- The school is aware that some users are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The Trust schools will all ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable users.
- The Trust schools will seek input from specialist staff as appropriate, including the SENDCo, Children Looked After lead, Wellbeing teams, Pastoral teams, multi agency teams etc.

Training and engagement with staff

The Trust schools will:

- Provide the Online Safety policy to all colleagues as part of induction.
- Provide up-to-date and appropriate online safety training, resources and updates for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to users (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with the Trust's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school. Please see our Social Media Policy for further information.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the users.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the school community.

Awareness and engagement with parents/carers

The Trust schools recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The Trust schools will build a partnership approach to online safety with parents/carers by:

- Providing information and guidance on online safety in a variety of formats.
- Drawing their attention to the Trust online safety policy and expectations in newsletters, letters, the prospectus and on the website.
- Requesting that they read online safety information as part of joining one of our schools, for example, within our home school agreements.
- Requiring them to read the AUPs and discuss its implications with their children.

Reducing Online Risks

The Trust schools recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- Regularly review the methods used to identify, assess and minimise online risks
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in schools is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a Trust computer or

device.

All members of the Trust community are made aware of the expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the AUPs and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom Use

The Trust schools use a wide range of technology. This includes access to:

- Computers, laptops and other digital devices.
- Internet which is likely to include search engines and educational websites.
- Email.

All Trust school owned devices will be used in accordance with the AUPs and with appropriate safety and security measures in place.

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home and check any data protection implications before using/implementing any online platform(s).
- The Trust schools will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- The Trust schools will ensure that the use of internet-derived materials, complies with copyright law and acknowledges the source of information.
- Supervision of learners will be appropriate to their age and ability.
- Learners will be appropriately supervised when using technology, according to their ability and understanding.

Projectors/Screens

We understand that many lessons will involve the use of a projector/screen. There are important security features that you must activate when you are accessing certain things, for e.g.:

1. The class register
2. Your emails (and anything linked to Gmail, for e.g. My Drive, shared with me etc).
3. CPOMS
4. Your home screen (you must be mindful of tabs that you may already have open). Your screen should not be shared until you have the resource on display (from your PC/laptop) that you want to share.

The screens/projectors that we use have a “freeze” feature. This allows you to pause whatever is currently being displayed on your screen, giving you the privacy you need to access your emails, class register etc without any unwanted displays.

On Epson projectors there is a button on the remote that says freeze and on Iiyama screens it's the blue button. Press once to freeze and again to unfreeze.

If you would like any help using this feature, please contact our Trust IT team on support@batleymat.co.uk.

Managing Device and Internet Access

- Access to Trust/school owned devices and resources is restricted to authorised users only.
- All staff, learners and visitors will need to read and accept the relevant AUPs before being given access to a device or resource.

Filtering and Monitoring Decision Making

- The Trust schools have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit exposure to online risks.
- The Trust and SLTs are aware of the need to prevent "over blocking", as that may unreasonably restrict what learners can be taught, with regards to online activities and safeguarding.
- The Trust schools' decision regarding filtering and monitoring has been informed by a risk assessment, taking into account the specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from SLT members.
- The SLT will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Filtering

- Please see Appendix A for each school's filtering system.

Dealing with Filtering breaches

- The Trust schools have clear procedures for reporting filtering breaches.
- If learners discover unsuitable sites, they will be required to secure and isolate the device and report any findings immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL/member of technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, West Yorkshire Police or CEOP.

Monitoring

- Each school will appropriately monitor internet use on all Trust owned or provided internet enabled devices. This may be achieved by: physical observation and supervision; device-based monitoring; internet activity monitoring. This may be in real-time, or by reviewing log files.
- The Trust schools all have a clear procedure for responding to concerns

identified via monitoring approaches. Any identified activity will be dealt with by the DSL as required.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Filtering and Monitoring Governance & Trust-Wide Annual Review

- Trust-wide alignment and rationale: the Trust recognises that statutory guidance (Keeping Children Safe in Education) recommends that reviews of filtering and monitoring effectiveness be conducted at an individual school level. However, because Batley Multi Academy Trust operates a centralised technical infrastructure with unified filtering and monitoring configurations applied across all Trust schools, the annual review of filtering and monitoring effectiveness is conducted strategically at Trust level.

- The annual Trust-wide review will be co-led by:
    1. A designated member of the Trust Central Team
    2. The Trust Safeguarding Lead (Trust Safeguarding Lead), in consultation with individual school DSLs and Headteachers.
    3. The Trust Director of IT

- Scope of Review & Site Verification: The central review will assess technical performance, filtering policy rules, blocked content logs, emerging threat trends, and local contextual safeguarding needs across all sites. To complement the central review, recorded physical and technical verification checks will be conducted annually on internet-connected devices across all individual school premises and locations, with written records retained centrally.

Managing Personal Data Online
- Personal data will be recorded, processed, transferred and made available online in accordance with Data Protection legislation.
- Full information can be found in the Data Protection Policy.

Security and Management of Information Systems
The Trust and all our schools take appropriate steps to ensure the security of our information systems, including:
- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus/malware scan before use.
- Not downloading unapproved software to work devices, opening unfamiliar email attachments or following unfamiliar internet links.
- Regularly checking files held on the school's/Trust network.

- The appropriate use of user logins and passwords to access the school/Trust network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All colleagues will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their passwords private.
- All learners are provided with their own unique usernames and private passwords to access school systems; they are responsible for keeping their passwords private.

We require all users to:

- Use strong passwords for access into our system. We recommend creating a passphrase comprising 3-4 random words as it serves as a lengthy yet easily memorable password.
- Always keep their passwords private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Managing the Safety of the School Website

- The Trust will ensure that information posted on our websites meets the requirements as identified by the Department for Education (DfE).
- The Trust will ensure that our websites comply with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Personal information will only be published on our websites, where this is statutory, or if consent has been given (where required); the details for the school will be the school address, email, telephone number and necessary contact information.
- The administrator account(s) for the Trust and school websites will be secured with an appropriately strong password.
- The Trust will post appropriate information about safeguarding, including online safety, on the school websites for members of the community.

Publishing Images and Videos Online

- The Trust and its schools will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to), the Data Protection and Safeguarding and Child Protection policies.

Managing Email

- Access to Trust school email systems will always take place in accordance with data protection legislation and in line with other relevant policies.

- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information should only be sent using secure and encrypted email.
- Members of the Trust community will immediately inform the DSL if they receive offensive communication.
- Excessive social email use can interfere with teaching and learning and may be restricted; access to external personal email accounts may be blocked in school.

Staff

- All members of staff (including Members, Trustees and Governors) are provided with a specific Trust/school email address, to use for all official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The use of Trust school email addresses for any personal reasons/activities is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when using email.

Learners

- Learners will use school provided email accounts for educational purposes only.
- Learners will agree to the AUP.

Social Media

Please refer to our Trust Social Media Policy for further information.

Use of Personal Devices and Mobile Phones

- The Trust schools recognise that personal communication through mobile technologies is an accepted part of everyday life for everybody, but technologies need to be used safely and appropriately within school settings. School policies for the use of mobile phones during working hours must be adhered to.
- Your personal mobile phone may be used as part of the 2FA process. Other methods of authentication are available via the Trust IT team.

Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate Trust and school policies.
- Electronic devices of any kind that are brought onto sites are the responsibility of the user at all times.
- All members of the Trust community are advised to take steps to protect their mobile phones or devices from loss, theft or damage. The Trust schools accept no responsibility for the loss, theft or damage of such items on school/Trust premises.

- All members of the Trust community are advised to use password/pin/biometric protection to ensure that unauthorised calls or actions cannot be made on their phones or devices; the sharing of these is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of the Trust community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene Behaviour or Safeguarding and Child Protection policies.
- Mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school sites such as changing rooms, toilets and swimming pools. School policies on mobile phones must be adhered to by staff at all times.
- The sending of abusive or inappropriate messages/content via mobile phones or personal devices *is not permitted by anyone.*

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant Trust/school policy and procedures.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson/working time.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled when not in use.
    - Not use personal devices during teaching periods, unless written permission has been given by the Headteacher or CEO for the central team, such as in emergency circumstances.
    - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents/carers.
- Any pre-existing relationships, which could undermine this, will be discussed with the DSL and/or Trust Headteacher or CEO.

Staff will not use personal devices to take photos or videos of learners. If a member of staff breaches any Trust/school policy in relation to personal devices, action will be taken in line with the relevant policies. If a member of staff is thought to have illegal content saved or stored on a personal device or have committed a criminal offence, the police will be contacted.

Learners' Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of

personal devices and mobile phones, and will be made aware of boundaries and consequences.
- The Trust schools expect learners' personal devices and mobile phones to be switched off and kept out of sight whilst in school.
- If a learner needs to contact a parent/carer, they will be allowed to use an appropriate school phone.
- Parents/carers are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by staff.
- Mobile phones or personal devices will not be used by learners during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by SLT.
- Mobile phones and other personal electronic or communication devices must not be taken into examinations.
- Learners found in possession of a mobile phone or other personal electronic or communication devices during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

Examining Electronic Devices
The Trust Headteacher, CEO and any member of staff authorised to do so by the Trust Headteacher or CEO, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting, in line with the latest DfE's guidance on screening, searching and confiscation:

- Poses a risk to staff or learners, and/or
- is identified in the school 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 learners and staff. If the search is not urgent, they will seek advice from the Headteacher or DSL.
- Explain to the young person why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the learner's cooperation.
- 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.

- Inform parents/carers.

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 school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the CEO, Trust Headteacher, DSL or SLT 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 learner and/or the parent/carers 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 learners 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
- The DfE's Searching, screening and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be addressed through the relevant complaints procedure.

Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and other visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the AUPs and other associated policies.
- The Trust schools will ensure appropriate signage and information is displayed/provided to convey the expectations.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL, SLT or CEO of any breaches of policy.

Trust school provided Mobile Phones and Devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/carers is required and there is no landline available.
- Trust school mobile phones and devices may be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Trust school mobile phones and devices must always be used in accordance with the AUPs and other relevant policies.

Responding to Online Safety Incidents and Concerns

- All members of the Trust community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, making or sharing of nudes and semi-nudes, cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official Trust/school procedures for reporting concerns.
- All members of the community will be informed of the complaints procedure and staff will be made aware of the whistleblowing procedure.
- The Trust requires all members of the community to work in partnership to resolve online safety issues.
- After any investigations are completed, the Trust school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the Trust is unsure how to proceed with an incident or concern, the local DSL will seek advice from the Kirklees Safeguarding Education Team.
- Where there is suspicion that illegal activity has taken place, the Trust will contact the Safeguarding Education Team or West Yorkshire Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the Trust community (for example if other local schools are involved or the public may be at risk), the school will speak with the Safeguarding Education Team or West Yorkshire Police first, to ensure that potential investigations are not compromised.

Concerns about Learner's Welfare

- The DSLs will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSLs will record these issues in line with the Safeguarding and Child

Protection policy.
- The DSLs will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kirklees Safeguarding Children Board thresholds and procedures.
- The school will inform parents/carers of any incidents or concerns involving their child, as and when required.

Staff Misuse
- Any complaint about staff misuse will be referred to the Trust Headteacher or CEO.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the relevant policies.

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children
- The Trust has accessed and understood the relevant part of Keeping children safe in education - GOV.UK.
- The Trust recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- The Trust recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The Trust also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The Trust will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHCE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If we are made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our relevant policies.
    - If content is contained on personal electronic devices, they will be managed in accordance with the DfE's searching, screening and confiscation advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting

and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions.
- Inform parents/carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
- If the concern involves children and learners at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with West Yorkshire Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Making or sharing of nudes and semi-nudes

- The Trust ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and making or sharing of nudes and semi-nudes.
- The Trust will implement preventative approaches via a range of age and ability appropriate educational approaches for all community members.
- The Trust views the consensual or non-consensual making or sharing of nudes or semi-nudes (encompassing self-generated imagery, content taken or created by others, and digitally altered or AI-generated content / deepfakes) as a critical safeguarding issue.
- The Trust will follow the guidance as set out in the non-statutory Sharing nudes and semi-nudes: advice for education settings working with children and young people
- If the Trust is made aware of incidents involving making or sharing of nudes or semi-nudes, the school will:
    - Act in accordance with the Safeguarding and Child Protection policy and the relevant Kirklees Safeguarding Children Board procedures.
    - Immediately notify the DSL.
    - Store any devices involved securely.
    - Carry out a risk assessment in relation to the young person/people involved.
    - Consider the vulnerabilities of learners/peoples involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for the learner(s), for e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Implement appropriate sanctions in accordance with the relevant policies but taking care not to further traumatise victims where possible.

    - Review the handling of any incidents to ensure that the school is implementing best practice and the Leadership Team will review and update any management procedures where necessary.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
    - Consider the deletion of images in accordance with the UKCIS guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- The Trust schools will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the DSL).
- The Trust schools will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school network or devices then the school will take action to block access to all users and isolate the image.
- The Trust schools will take action regarding creating youth produced sexual imagery, regardless of the use of Trust equipment or personal equipment, both on and off the premises.
- The Trust schools will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- The Trust ensures that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The Trust will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for all members of the community.
- The Trust views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.
- If the Trust is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Kirklees Safeguarding Children Board or the Police.
- If the Trust is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed to the DSL.

If the Trust is made aware of incidents involving online child sexual abuse of a child then it will:

- Act in accordance with the Safeguarding and Child Protection policy and the relevant Kirklees Safeguarding Children Board procedures.
- Immediately notify the DSL.

    - Store any devices involved securely.
    - Immediately inform the Police via 101 (using 999 if a child is at immediate risk)
    - Where appropriate the school will involve and empower learners to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
    - Carry out a risk assessment in relation to the learner(s) involved.
    - Consider the vulnerabilities of the learner(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for the learner(s), for e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- The Trust schools will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The Trust schools will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If young people at other schools are believed to have been targeted then it will seek support from Kirklees' Education Safeguarding Team to enable other schools to take appropriate action to safeguard their community.
- The Trust schools will ensure that the Click CEOP report button is visible and available to learners and other members of the school community, for example including the CEOP report button on the safeguarding pages of the school's websites.

Indecent Images of Children (IIOC)

- The Trust ensures that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The Trust will take action regarding Indecent Images of Children (IIOC) regardless of the use of Trust equipment or personal equipment, both on and off the premises.
- The Trust will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the Trust is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Kirklees Safeguarding Children Board or the Police.

If the Trust is made aware of Indecent Images of Children (IIOC) then it will:

- Act in accordance with the Child Protection and Safeguarding policy and

the relevant Kirklees Safeguarding Children Board procedures.
- Immediately notify the DSL.
- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), the Police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

If the Trust is made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children whilst using the internet then the Trust school will:

- Ensure that the DSL is informed.
- Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure access to the URLs is blocked on the local internet filtering systems.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents/carers.

If the Trust is made aware that indecent images of children have been found on the school's electronic devices then the school will:

- Ensure that the DSL is informed.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents/carers.

If the Trust school is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the Trust, then it will:

Ensure that the DSL is informed or another member of staff in accordance with the Trust whistleblowing procedure.
- Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
- Follow the appropriate Trust policies regarding conduct.

Cyberbullying
Cyberbullying 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 each school's relevant anti-bullying policy for further information).

- Cyberbullying, along with all other forms of bullying, of any member of the Trust community will not be tolerated.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the Trust community affected by online bullying.
- If the Trust is unclear if a criminal offence has been committed, then the DSL will obtain advice immediately through the Kirklees Safeguarding Children Board or the Police.
- All members of the community will be advised to keep a record of cyberbullying as evidence.
- The Trust will take steps to identify the bully where possible and appropriate. This may include examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- All members of the community will be required to work with the Trust to support the approach to cyberbullying and the online safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended for the user for a period of time. Other sanctions for young people and staff may also be used in accordance with the relevant policies.
    - Parents/carers of those involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Online Hate

- Online hate at the Trust schools will not be tolerated.
- All incidents of online hate reported to the Trust schools will be recorded.
- All members of the community will be advised to report online hate.
- The Police will be contacted if a criminal offence is suspected. If the Trust school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Kirklees Safeguarding Children Board or the Police.

Online Radicalisation and Extremism

- The Trust schools will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school, and that suitable filtering is in place which takes into account the needs of all young people.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with the Safeguarding and Child Protection policy.

- Online hate content directed towards or posted by specific members of the community will be responded to.
- If the Trust school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Kirklees Safeguarding Children Board or the Police.
- If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher or CEO will be informed immediately, and appropriate action will be taken.

Appendix A - Solutions in use across the Trust

This is a school breakdown of the filtering and monitoring solutions deployed across the school sites

School	Filtering Solution	Monitoring Solution
Batley Girls' High School	Lightspeed	Classroom. Cloud/NetSupport
Batley Grammar School	Lightspeed	Classroom. Cloud/NetSupport
Field Lane Junior, Infant and Nursery School	Lightspeed	Classroom. Cloud/NetSupport
Healey Junior, Infant and Nursery School	Lightspeed	Classroom. Cloud/NetSupport
Manorfield Infant and Nursery School	Lightspeed	Classroom. Cloud/NetSupport
Upper Batley High School	Lightspeed	Classroom. Cloud/NetSupport
Purlwell Infant and Nursery School	Lightspeed	Classroom. Cloud/NetSupport
Hyrstmount Junior School	Lightspeed	Classroom. Cloud/NetSupport

Accurate at the time of publication.

Appendix B - Contacts List

Online Safety (e-Safety) Contacts and References
Kirklees Safeguarding Children Board:
www.kirkleessafeguardingchildren.co.uk/safeguarding_education.html

Kirklees Safeguarding Education Team
Email: schoolsafeguardingofficer@kirklees.gov.uk OR telephone number: 01484 221919

West Yorkshire Police: www.westyorkshire.police.uk
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact West Yorkshire Police via 101.

Kirklees Police Safeguarding Unit
Email: ea.safeguarding@westyorkshire.pnn.police.uk OR telephone number: 01924 335073

West Yorkshire Police links:
Child sexual exploitation advice for adults – www.westyorkshire.police.uk/cse

Online grooming
www.westyorkshire.police.uk/advice/online-crime-safety/online-safety/cyber-crime/on line-grooming-child-sexual-exploitation

Sexting –

www.westyorkshire.police.uk/sexting *Other*

Local Safeguarding Children Boards Bradford –

www.bradford-scb.org.uk Calderdale –

www.calderdale-scb.org.uk

Leeds – www.leedslscb.org.uk

Wakefield – www.wakefieldlscb.org.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Online Compass (Self review tool for other settings)**:**
http://www.onlinecompass.org.uk/

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

UK Safer Internet Centre: www.saferinternet.org.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Appendix C - Colleague ICT Acceptable Use Policy

Batley Multi Academy Trust (The Trust) provides ICT and communications equipment for use by colleagues, visitors, volunteers, trainees etc. (referred to as staff), as an important tool for teaching, learning, personal development and administration of each school within the Trust. Use of these facilities is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to ICT Support staff in your school in the first instance.

All colleagues have a responsibility to use each school's technology facilities in a professional, lawful, and ethical manner. Deliberate abuse or misuse of the computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability. Please note that use of these facilities is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines.

This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the Trust and staff, to safeguard the reputation of the Trust, and to ensure the safety of all users.

Please respect these guidelines, many of which are in place for your protection. The Trust recognises that the distinction between ICT use at work and at home is increasingly blurred, with many of us now using our own equipment for work. While the Trust neither wishes nor intends to dictate how you use your own technology, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the Trust.

Device Security and Data Protection

- You will be provided with a personal school/Trust account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, you must not disclose your password to anyone, including ICT support staff. If you do so, you will be required to change your password immediately.
- You must not allow a young person to have use of a staff account under normal circumstances. The only exception is when using an interactive whiteboard in lesson tasks and the learner is supervised at all times.
- When leaving a computer unattended, even for a short period, you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence. Failure to do this will be considered a serious breach of security and may lead to a data breach.
- USB storage devices are not permitted in our Trust.
- You must not store any sensitive or personal information about colleagues or learners on any portable storage system (such as a USB storage device, portable hard disk, or personal computer/laptop/device).

- You must not transmit any sensitive or personal information about staff or learners via email outside the Trust schools' systems without the data being encrypted or appropriately protected.
- If you use a personal computer at home for work purposes, you must ensure that any Trust-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.
- You should not make your own backup of data kept on any storage system other than the network storage drives or your 'My Documents' folder. This includes USB memory sticks (even those owned or issued by the Trust), laptops or a personal computer.
- You should ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
- Equipment taken off site is not routinely insured. If you take any Trust school equipment off site, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft. Please discuss this with the relevant member of staff.

Personal Use

- Trust devices and/or equipment cannot be used for personal use.
- Trust devices and/or equipment cannot be loaned to any other person.

Use of your own Equipment

- Any mains-operated personal device or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by the Trust's normal rules on electrical safety testing.
- You must not connect personal devices equipment to the Trust schools' computer equipment without prior approval from the relevant IT staff.
- Personal mobile phones or other personal electronic equipment must not be used to take photos or videos of learners.

Conduct

- You should avoid eating or drinking around computer equipment.
- All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP) in addition to the guidelines here.
- Staff should not use their own personal email address or personal phone number when contacting parents/carers.
- Staff should not use the Trust's printing facilities for non-work related materials without seeking permission, and agreeing to pay for such use if applicable.
- You must at all times conduct your computer usage professionally, which includes using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:

    - Using, transmitting, or seeking inappropriate, offensive, pornographic,

vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials.
    - Making slurs or jokes relating to the 9 protected characteristics in the Equality Act 2010.
    - You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.
    - You should not intentionally damage, disable, or otherwise harm the operation of computers.
    - You should make efforts not to intentionally waste resources. Examples of resource wastage include:
        - Excessive downloading or streaming of material or services from the Internet (especially for non-curriculum purposes).
        - Excessive storage of unnecessary files on the network storage areas.
        - Use of computer copiers to produce class sets of materials, instead of using reprographics.

Use of social networking sites, blogs, forums and non-school emails
Staff must take care when using social networking websites such as, but not limited to, TikTok, Facebook, X, SnapChat, Instagram, LinkedIn etc. Social networking sites promote informal relationships and increased sharing of personal information. As such they can leave you open to abuse. Please see our Social Media Policy for further information on our expectations on the use of social media and how to keep yourself safe online.

Use of Email
All members of staff are provided with an individual email address for communication both internally and with other email users outside the Trust schools. The following considerations must be made when communicating by email:

- Email has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of emails may therefore have to be made available to third parties. You should be cautious when sending both internal and external mails. The professional standards that apply to internal, external letters and all forms of communication must be observed for email.
- Email to outside organisations has the same power to create a binding contract as hardcopy documents. Check emails as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You may not purchase goods or services on behalf of the Trust schools via email without proper authorisation.
- All emails should have a signature containing your name, job title and the name of the school.
- Email can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you should not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential

information belonging to the Trust schools.
- Having an external email address may lead to receipt of unsolicited email containing offensive and/or sexually explicit content. The Trust schools will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the internet.
- You should not use the email account provided by the Trust schools to send private or personal messages, including signing up to sites or services that are not work related.
- You must not send chain letters or unsolicited commercial email (also known as SPAM).

Supervision of Learners' Use
- Learners should be supervised at all times when using school computer equipment. When arranging use of computer facilities for learners, you should ensure supervision is available.
- Supervising staff should ensure they have read and understand all relevant policies prior to supervising a young person.

Confidentiality and Copyright
- Respect the work and ownership rights of people outside the Trust schools, as well as other staff or learners.
- You are responsible for complying with copyright law and licences that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the computer system or the internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- You should consult the relevant member of staff before placing any order for computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase/use may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the Trust schools' systems.

Reporting Problems with the Computer System
It is the job of ICT support for each school and the Trust to ensure that the computer system is working optimally at all times and that any faults are rectified as soon as possible.

To this end:
- Please report any problems that need attention to a member of ICT support staff as soon as possible using the recommended methods. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone or radio; any other problem should be reported via the relevant process.
- If you suspect your computer has been affected by a virus or other malware,

please report this to a member of ICT support staff immediately. Virus software may pop up a warning which should not be ignored.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Privacy
- Use of the computer system, including your email account and storage areas provided for your use, is subject to monitoring by the Trust schools to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the Trust/school may keep a record of sites visited on the internet by both young people and staff, however, passwords used on those sites are not monitored or recorded.
- You should avoid storing any sensitive personal information on the computer system that is unrelated to work related activities (such as personal passwords, photographs, or financial information).

Reporting Breaches of this Policy
All members of staff have a duty to ensure this Acceptable Use Policy is followed. You should immediately report abuse of any part of the computer system.

In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or learners.
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.
- Any breaches, or attempted breaches, of computer security or AUPs.
- Any instance of bullying or harassment suffered by you, another member of staff, or a learner via the Trust schools' computer system.

All reports will be treated confidentially.

Confirmation of Agreement
By using any Trust school device, service or resource, you acknowledge agreement with this AUP, and to abide by it. You may be asked electronically to confirm your agreement so it can be recorded.

Appendix D - Learners' ICT Acceptable Use Policy

ICT access is now fundamental to the learners' curriculum delivery development of core skills. This includes access to various devices, email (dependent on age and setting), various online platforms, the ability to store work on the school system and online. Learners will be able to exchange email with staff and peers for learning purposes, and may have some details uploaded to online platforms in line with relevant data sharing agreements and data protection legislation.

The Trust schools operate internet filtering systems which are regularly updated to help prevent access to inappropriate sites, but schools are moving towards a model of education and discussion rather than just simple blocking (adult, illegal and other such content is always blocked where possible).

Please find below a copy of the Learners' Acceptable Use Policy for School ICT systems (devices, software, platforms, storage, internet, email, printers etc) policy.

Learners' Acceptable Use Policy for School ICT systems (devices, software, platforms, storage, internet, email, printers etc) policy.

The Trust schools computer systems, devices, and online platforms it uses are provided to help learners further their education and for staff to enhance their professional activities including teaching, learning, research, administration and management.

This agreement has been drawn up in line with our safeguarding policies.

- In all cases, use of the ICT system is reserved for education purposes only. Use of ICT for any use other than that directly related to school work is not permitted.
- Use of ICT resources may be monitored at any time, this includes stored files, internet use, emails and printed work.
- Under no circumstances should you share your logon details (username and password), or leave a computer unattended whilst you are logged on.
- Users must not attempt to make any change to ICT software or hardware. This includes the removal/addition of any cables relating to ICT equipment. This also includes attempts to bypass any security or monitoring systems that may be in place.
- All legal copyrights must be respected and adhered to, this includes not downloading or storing music and video from the internet which is copyrighted.
- Attempts to access adult, illegal or other offensive material is not allowed.
- Images (photo or video) of learners, staff, school or community will not be used in any way without the relevant consent.

By using any device or system provided to you by your school, you understand the use of the ICT systems is granted in accordance with the above, and that any use may be monitored. Any misuse or failure to abide by the policy, may result in privileges being withdrawn, and standard school disciplinary procedures being followed. Online

platform providers may have their own agreements which the Trust/ school has reviewed, but learners also should be aware of these. They are available on request.

Our learners will be presented with this AUP prior to accessing any system - this will be displayed electronically.