Online Safety Policy

Version	Version 1.0.0
Review Date	September 2023
Next review	September 2024

Contents

Scope Of Policy 3
Roles and Responsibilities 4
Head Teacher, DSL and Senior Leaders 4
Online Safety Lead (if applicable to school structure) 5
All School Staff, Governors and Volunteers 6
PSHRE and Computing Leads 6
Local Governing Committees 6
Pupils 6
Parents 7
Trust ICT Team 7
Education of Pupils 8
Education and information for Parents and Carers 9
Training of Staff and Governors 10
Unacceptable online activity including child on child abuse 10
Cyberbullying 10
Sexting 11
Sexual Harassment, including Upskirting 11
Prevent 12
Appropriate Filtering of Internet Connections 12
Appropriate Monitoring of Internet Connections 13
Assessment of Risk 13
Reporting 14
Use of Digital Images & Sound 15
Communication 16
With respect to email and other online communication tools (e.g. Microsoft Teams, Google Meet) 16
With respect to Online/Remote Learning e.g. Microsoft Teams, Google Classroom, Seesaw, Tapestry etc. 16
Sanctions and Disciplinary Proceedings 20
Appendix A: Action to take in response to inappropriate use 21
Appendix B: Information for Parents Template 22
Appendix C: Methods of Communication 24

Scope Of Policy

The purpose of this policy is to support the safeguarding of children whilst accessing the internet in school and applies to all members of the school community, including staff, pupils, governors, visitors parents/carers, visitors and community users.

Keeping Children Safe in Education 2023 sets out and strengthens specific responsibilities for Schools, Trusts and Local Governing Committees. Online safety is now considered part of everyone's statutory safeguarding responsibilities and requires a whole-school approach including:

- Children are taught about online safety
- Appropriate filtering and monitoring systems are in place
- Online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach
- DSL understanding of filtering and monitoring systems

In addition to the responsibilities of KCSIE the Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but are linked to membership of the school. It applies to both staff and pupil use of technology for learning.

Trust schools will manage Online Safety as described within this policy. Schools inform parents and carers of known incidents of inappropriate Online Safety behaviour that take place in and out of school.

This Online Safety Policy should be read in conjunction with the following Trust and School level policies:

- Safeguarding and Child Protection Policy
- Behaviour Policy (School Policy)
- Acceptable Use Policies for Staff, Governors and Volunteers
- Acceptable Use for Pupils & Parents (Trust Template Policies for Schools to edit)
- Data Protection Policies
- Trust ICT Security Policy
- Consent forms for data sharing, image use etc (School Policies)

Roles and Responsibilities

In each school the Designated Safeguarding Lead and Local Governing Committee (LGC) oversee the safe use of technology when children and learners are in their care. Head teachers and DSL's act immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being.

Head Teacher, DSL and Senior Leaders

The Head teacher is responsible for ensuring practice, procedure, systems and training is implemented to safeguarding children and members of the school community online, this includes the PREVENT duty to stop individuals being drawn into terrorism.

KCSIE 2023 states that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)". The Designated Safeguarding Lead (DSL) will have an overview of the serious child protection issues that can arise from online access, including: sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation, inappropriate online contact with adults, cyber-bullying and potential or actual incidents of grooming and these will be recorded.

The Head teacher/DSL has the following responsibilities:

- Have a high level understanding of the functionality of the Trusts filtering and monitoring systems.
- Understand the limitations of filtering and monitoring technologies and have processes in place within school to mitigate risks.
- Be able to investigate alerts and reports within the filtering system.
- Ensure that all staff receive suitable professional development to carry out their Online Safety roles including online risks of extremism and radicalisation and are aware of the procedures outlined in policies relating to Online Safety
- Create a culture and processes where staff and learners feel able to report incidents
- In collaboration with the schools PSHE/RSHE, Computing Leads and other Trust Online safety leads embed and monitor a progressive Online Safety curriculum for pupils (as part of the RSE Curriculum and to reinforce and extend learning within the Computing Curriculum)
- Ensure that Online Safety incidents and reports are monitored at school level. Log, manage and inform others of Online Safety incidents and how they have been resolved where this is appropriate
- Follow correct safeguarding procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil
- Inform the Trust and local authority about any serious Online Safety issues
- Report issues with school infrastructure & networks to the Trust ICT manager to ensure that it is as safe and secure as possible
- Ensure that policies and procedures approved within this policy are implemented
- Review the Online Safety with the 360 online safe tool provided by the SWGFL and Trust (with support from the DSL and Trust ICT Team) every 18 months.

- Inform Parents and Carers of the filtering & monitoring systems that the Trust/School use so that they can understand how we work to keep children safe.
- Inform Parents & Carer of the online curriculum, including sites that they need to access and with whom they will be interacting online (See the template in Appendix B)
- Work with the DSL, Online Safety Lead, Trust ICT Manager and Data Protection Officer to ensure that the remote learning strategy developed and implemented by the school meets safeguarding and online safety requirements
- Attend updates and training provided by the Trust ICT Team and School Improvement Team
- Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments
- Provide and/or broker training and advice for staff and attend Trust ICT training on the use of the Trust filtering and monitoring systems
- Coordinate work with the school's Online Safeguarding Lead (OSL) where the school structure includes an OSL
- Read and understand the Trusts Online Safety policy and documents and contribute to their review through the Trust ICT strategy group.
- Work with the OSL and Data Protection Officer to ensure that the Remote/Online Learning strategy developed and implemented by the school meets safeguarding and online safety requirements

Online Safety Lead (if applicable to school structure)

- Have a high level understanding of the functionality of the Trusts filtering and monitoring systems.
- Understand the limitations of filtering and monitoring technologies and have processes in place within school to mitigate risks.
- Be able to investigate alerts and reports within the filtering system.
- Coordinate work with the school's Head Teacher/Designated Safeguarding Lead (DSL)
- Monitor and inform the DSL of Online Safety incidents involving Pupils
- Read and understand the Trusts Online Safety policies and documents and contribute to their review through the Trust ICT strategy group.
- In collaboration with the schools PSHE/RSHE, Computing Leads and other Trust Online safety leads embed and monitor a progressive Online Safety curriculum for pupils (as part of the RSE Curriculum and to reinforce and extend learning within the Computing Curriculum)
- Work with the DSL, Headteacher and Data Protection Officer to ensure that the Remote/Online Learning strategy developed and implemented by the school meets safeguarding and online safety requirements
- Ensure all staff are aware of the procedures outlined in policies relating to Online Safety
- Provide and/or broker training and advice for staff
- Attend updates and training provided by the Trust ICT Team and School Improvement Team
- Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments
- Be the first point of contact within school for reporting issues with filtering
- Attend Trust ICT training on the use of the Trust filtering and monitoring systems
- Assist with managing and maintain the schools local filtering lists for the school

If a school does not have an Online Safety Lead, all responsibilities within this role are moved to the Designated Safeguarding Lead.

All School Staff, Governors and Volunteers

- Participate in any training and awareness raising sessions
- Read, understand, sign and act in accordance with the Trust Staff and Volunteers Acceptable Use Policy and Online Safety Policy
- Report any suspected misuse or concerns (within or outside school) to the Online Safety Lead and/or Designated Safeguarding Lead (DSL) and check this has been recorded and actioned
- Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum
- Model the safe, positive and purposeful use of technology
- Monitor the use of technology in lessons, extracurricular and extended school activities, including Online/Remote Learning
- Be mindful of the additional safeguarding considerations required if delivering Online/Remote Learning
- Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident

PSHRE and Computing Leads

- Work with the Curriculum Leads to embed and monitor a progressive Online Safety curriculum for pupils. Deliver this as part of the RSE Curriculum and to reinforce and extend learning within the Computing and wider school curriculum.

Local Governing Committees

LGCs have the following responsibilities:

- Monitor the effectiveness of the Online Safety Policy[1].
- Appoint a Safeguarding Lead governor to work with the school's Designated Safeguarding and Online Safety Leads to carry out regular monitoring and report to Governors.
- To verify that the filtering, monitoring and or supervision systems are in place to identify children accessing or trying to access harmful and inappropriate content online.

Pupils

[1] Online safety in schools and colleges: Questions from the Governing Board

- Read, understand, sign (where appropriate) and act in accordance with the Pupil Acceptable Use Policy and/or agreed class appropriate use of technology agreement
- Report concerns for themselves or others
- Make informed and positive choices when using technology in school and outside school, considering the effect on themselves and others

Parents

- Endorse the Parent & Child Acceptable Use Policy (this should be an electronic form)
- Discuss appropriate, healthy, safe use of technology and Online Safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the internet.
- Inform the Head teacher of any Online Safety concerns.
- Use formal channels to raise matters of concern about their child(ren)'s education.
- Maintain responsible standards when referring to the school on social media as agreed in the Parent & Child Acceptable Use Policy.

Trust ICT Team

- Monitors the Trust ICT team actions and projects to ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack as defined in the Trust ICT Security policy.
- Ensure users may only access school systems using an approved password
- Provide Online/Remote learning platforms that meet safeguarding and online safety requirements
- Ensure curriculum platforms used by the school meet online safety, security and UK GDPR requirements
- Maintain and inform the Trust Senior Leadership Team of issues relating to online safety
- Audit changes made to filtering systems by Trust ICT and school staff.
- Monitor Internet access and filtering across all schools at Trust level.
- Ensure alerts are sent to schools should an online safety incident occur
- Collaborate with Head teachers /OSLs and DSLS's to investigate online safety incidents where appropriate.
- Keep up to date with Online Safety technical information.
- Update and train school staff on online safety and systems.
- Ensure use of the Trust's network is regularly monitored in order that any misuse can be reported to the appropriate Online Safety Lead/Designated Safeguarding Lead for investigation
- Ensure monitoring and filtering systems are implemented and updated
- Ensure that the Trust ICT security policy is followed
- Sign an extension to the Staff Acceptable use Policy detailing any extra responsibilities in regards to online safety.

- Sign the Trust ICT Staff AUP in addition to the general Staff AUP which includes agreements on how technical systems and services are accessed and used.

Trust Senior Leadership

- Have a high level understanding of the functionality of the Trusts filtering and monitoring systems.
- Understand the limitations of filtering and monitoring technologies and have processes in place within school to mitigate risks.
- Be able to investigate alerts and reports within the filtering system.
- Create a culture and processes where staff feel able to report incidents
- Ensure that Online Safety incidents and reports involving head teachers and central team members are monitored at Trust level by at least:
    - 2 members of the ICT/Operations Team
    - 1 member of the School Improvement Team
    - 1 member of the HR team
- Log, manage and inform others of Online Safety incidents and how they have been resolved where this is appropriate
- Follow correct safeguarding procedure in the event of a serious Online Safety allegation being made against a member of staff
- Inform the Trust and local authority about any serious Online Safety issues
- Ensure that policies and procedures approved within this policy are implemented
- Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments
- Read and understand the Trusts Online Safety policy and documents and contribute to their review through the Trust ICT strategy group.
- Sign the Trust ICT Staff AUP in addition to the general Staff AUP which includes agreements on how technical systems and services are accessed and used.

Education of Pupils

Keeping Children Safe In Education states the following responsibility for schools:

'Children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum'

All Trust Schools provide a progressive and planned Online Safety education programme that takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured through reference to UK Council for Internet Safety Education for a Connected World framework.

Within this:

- Key Online Safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all teaching.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage Pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Within lessons where internet use is pre-planned Pupils are guided to sites checked as suitable for their use in advance and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- The Online Safety Lead maintains and passes on knowledge of current concerns to be included within learning experiences.
- Pupils will write and sign an Acceptable Use Policy for their class at the beginning of each school year.
- Pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying' and given opportunities to support each other.
- A continuous provision map is used with the youngest learners and SEN learners to establish appropriate habits for responsible use of technology.

Education and information for Parents and Carers

Parents and carers will be informed about the ways the internet and technology is used in school and sign the Trust Parent and Pupil acceptable use policy on behalf of themselves and their child.

Parents and Carers have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The Trust and it schools support parents and carers to do this by:

- Providing clear Acceptable use guidance which they are asked to agree to for their children (The Trust provide a template for all schools for Pupils & Parents).
- Providing regular newsletter items and appropriate support materials*
- Raising awareness through activities planned by pupils and staff
- Inviting parents to attend activities such as Online Safety week, Online Safety assemblies or other meetings as appropriate
- Maintaining up to date information on the School and Trust websites

The Trust ICT Team signpost useful support materials for schools to use on the Trust ICT support site (http://trustict.bwmat.org).

Resources for parents and children about online safety are available at: Keeping children safe online | NSPCC

Training of Staff and Governors

Schools must plan a programme of Online Safety training as part of the overarching safeguarding approach, in line with Keeping Children Safe 2023 for all staff and governors to ensure they understand their responsibilities, as outlined in this document and the Acceptable Use Policies. This includes:

- All staff knowing the Designated Safeguarding Lead and the Online Safety Lead and their responsibilities.
- An annual audit by the school of the Online Safety training needs of **all** staff.
- All new Staff and Governors receiving Online Safety training on Educare as part of their induction programme, ECTs will be supported to complete the UKCIS Online Safety Audit Tool.
- Providing information to supply and Pupil teachers on the school's Online Safety procedures.
- the Online Safety Lead receiving regular updates through attendance at training sessions provided by the Trust and by reviewing Online Safety newsletters from the Trust ICT SharePoint site (3 newsletter are published each year).
- This Online Safety Policy and annual updates being shared and discussed in staff meetings and in Governor meetings.
- The Online Safety Lead or Designated Safeguarding Lead providing training within safeguarding training and as specific online safety updates and reviews.
- The Online Safety Lead providing guidance as required to individuals and seeking Trust and LA support on issues
- Staff and Governors are made aware of the Professionals Online Safety Helpline (POSH) 0344 381 4772
- Parents will sign the Trust Parent and Pupil acceptable use policy on behalf of themselves and their child.
- Staff will attend Trust ICT Team provided training in the use of Filtering and Monitoring Systems for Designated Safeguard Leads, ICT Coordinators and Online Safety Leads (and refresher courses) annually.

Unacceptable online activity including child on child abuse

All members of the school community are made aware that children could abuse other children. All schools will ensure that staff are aware of the Trust's Child Protection and Safeguarding policy. This policy does not define the investigation of child on child abuse but does define the actions that should be taken to encourage the reporting of incidents and those to be taken alongside investigation.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

- Pupils and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by; telling a trusted adult, Online bully box, Childline App and phone number 0800 1111, Professionals Online Safety Helpline: 0344 381 4772.
- Pupils, staff and parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.
- All incidents of online bullying reported to the school will be recorded and action taken by the school.
- The school will follow procedures in the Trust's CP and Safeguarding policy to investigate incidents or allegations of online bullying.
- The school will take steps where possible and appropriate, to identify the perpetrator. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the Trust ICT Team and the police.
- Pupils, staff and parents and carers will be required to work with the school to support the approach to online bullying and the school's Online Safety ethos.
- Sanctions for those found to be involved in online bullying will follow those for other bullying incidents as indicated in the schools Behaviour Policy and AUP and may include:
    - The perpetrator being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content
    - ICT access being suspended at school for a period of time.
    - ICT access to school systems being suspended outside of school
    - the parent and carers of pupils being informed
    - the police being contacted if a criminal offence is suspected

Sexting

Trust schools will follow UKCIS advice on how to respond to any incident of sexting. The school will provide appropriate support for sexting incidents which take place in and out of school. **Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off.** This will then be reported to the Designated Safeguarding Lead (DSL), LADO and Police. The DSL will report to the LADO and Police. An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) will record any incident of sexting and the actions taken in line with advice from the Trust's Education and Trust ICT Teams.

Sexual Harassment, including Upskirting

All staff are made aware that sexual harassment can occur between two children of any age and sex and can include online harassment. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence and can include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- unwanted sexual comments and messages, including, on social media
- sexual exploitation; coercion and threats
- upskirting

All staff are made aware of what upskirting is, and that it is illegal. Any incident of sexual harassment will be taken seriously and reported to the Designated Safeguarding Lead (DSL). The Designated Safeguarding Lead (DSL) will record the incident(s) and the actions taken in line with the Trust Safeguarding Policy, DFE Guidance in KCSIE and/or the police as necessary.

Prevent

The Trust and its schools work to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place. DSLs should refer to the Trusts Safeguarding and Child Protection policy for further guidance and actions.

Appropriate Filtering of Internet Connections

The Trust ICT service provide all schools with a platform to appropriately filter and monitor Internet access based upon age and role within the school ('NetSweeper')

Recognising that no filter can guarantee to be 100% effective, the Trust filtering system manages the following content (and web search).

Content	Note
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
Drugs & Substance Abuse	Displays or promotes the illegal use of drugs or substances
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance
Malware/Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	Displays sexual acts or explicit images
Piracy and copyright Theft	Includes illegal provision of copyrighted material
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)
Violence	Displays or promotes the use of physical force intended to hurt or kill
Illegal activity	IWF Filter lists for Child Sexual Abuse Material & the Home Office Police assessed list of unlawful terrorist content

This list is not exhaustive and in addition, Schools may choose to filter and block any Internet content where it impedes or is detrimental to Teaching and Learning.

The Trust retain logs of Internet access of all pupils for 6 months. All school owned devices (including any SEN provisioned devices treated as part of the schools IT estate) will filter internet access on any internet connection (at work and at home) and are therefore have the potential to be monitored.

Appropriate Monitoring of Internet Connections

The Trust ICT service provide all schools with a platform to appropriately filter and monitor Internet access based upon age and role within the school ('NetSweeper')

Netsweeper will alert school DSLs and Online Safety leads to potential causes for concern.

The Trust ICT Team have scheduled reports and alerts that will be sent automatically.

Where a cause for concern relates to a Head Teacher or Central Team Member, the Trust Chair of Governors and Chief Executive will be alerted via email automatically.

Monitoring systems require capable and competent staff with sufficient capacity to effectively manage them, together with the support and knowledge of the entire staff. Monitoring systems are there to safeguard children and the responsibility therefore lies with the school leadership/governors and Designated Safeguarding Lead. Schools should ensure that their staff and in particular those responsible for and managing their monitoring strategy have sufficient capacity and capability.

Automated Monitoring Alerts and Reports

Each week the DSL will receive separate reports detailing search terms and websites blocked for staff, pupils and guest devices within the school. These are sent to the safeguarding@xxxxx.bwmat.org email address and the SLT-Confidential group for each school.

Each week the OSL will receive reports detailing search terms and websites blocked for pupils within the school. These are sent to the studentinternetmonitoring@xxxxx.bwmat.org account.

Where monitoring detects a significant risk and instant Alert will be sent. Alerts in regards to Adult use are sent to the safeguarding@xxxxx.bwmat.org and SLT-Confidential Groups. Alerts for Pupils are sent to safeguarding@xxxxx.bwmat.org, SLT-Confidential and the OSL studentinternetmonitoring@xxxxx.bwmat.org account.

Assessment of Risk

Methods to identify, assess and minimise risks will be reviewed annually at Trust level and every 18 months at school level using the 360 safe assessment. As technology advances the Trust will examine and adjust the Online Safety Policy. Part of this consideration will include a risk assessment including the Trust ICT manager:

- looking at the educational benefit of the technology

- considering whether the technology has access to inappropriate material

The Trust are the ultimate authority for decisions relating to technology procurement (as stated in the Scheme of Delegation and Trust ICT strategy documents)

The Trust provides appropriate filtering and monitoring as stated in this policy. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school device.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting

The Trust and school will respond to illegal and inappropriate incidents with advice from the POSH helpline and LADO. More than one member of school staff (at least one should be a senior leader) and a member of the Trust School Improvement Team will be involved in this process. The Trust School Improvement Team will use the resources of the Trust ICT manager when appropriate. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. **Where content being reviewed is suspected or known to include images of child abuse, the investigation will be referred to the Police immediately and no further access will be made by the school to the material.**

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content).
- Staff will record incidents in CPOMS. All reported incidents will be dealt with and actions recorded
- The school will inform the Trust ICT Team and Education team, who will assist with any investigation.
- The Designated Safeguarding Lead (DSL) will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures
- The school will manage Online Safety incidents in accordance with the School Behaviour and Trust Safeguarding & Child Protection Policies where appropriate
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- After any investigations are completed, the Trust and school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the appropriate LADO and local authority safeguarding team and escalate the concern to the police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Education Safeguarding Service or Local Authority Designated Officer (LADO).

The police will be informed immediately where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images.
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation.
- adult material that potentially breaches the Obscene Publications Act in the UK.
- criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false.

Use of Digital Images & Sound

Photographs, video and sound recorded within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- build a culture where permission is always sought before a photo is taken or video and sound are recorded; including encouraging pupils to seek permission from other pupils to take, use, share, publish or distribute images and sound.
- ensure verifiable permission from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on the school website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use.
- when using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images, record video and sound to support educational aims, following the school policy regarding the sharing, distribution and publication of those. School equipment only is used. Personal equipment of staff is not allowed for this purpose.
- make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed.
- ensure that pupils' full names will not be used anywhere on the school website, school blogs or within school branded social media, particularly in association with photographs
- not publish pupils' work without their permission and the permission of their parents or carers.
- only hold digital/video images on school approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the schools Data Retention Policy.
- in accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at school events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video

images or in the sound recording. Schools will ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before each event as to the expectations of the school.

- make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the settings Online Safety Policy and will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people.

Communication

A wide range of communications technologies increases effective administration and has the potential to enhance learning.

With respect to email and other online communication tools (e.g. Microsoft Teams, Google Meet)

The Trust ICT team provide secure business systems for communication in line with the Trusts ICT Security Policy.

Trust schools will:

- ensure that staff and governors use these secure business systems for communication in accordance with the Staff and Volunteers AUP.
- ensure that personal information is not sent via unsecure systems.
- ensure that governors use secure systems.
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content.
- make users aware that communications will be monitored by the school and Trust ICT Team.
- inform users what to do if they receive online communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- teach pupils about email and other communication tools alongside safe, healthy appropriate use of technology and online safety issues through the scheme of work and implementation of the school's Parent and Pupil AUPs
- only publish official staff email addresses where this required
- protect the identities of multiple recipients by using bcc in emails

With respect to Online/Remote Learning e.g. Microsoft Teams, Google Classroom, Seesaw, Tapestry etc.

The Trust provides Teams, Google and Apple Classroom platforms consistently across all schools

Trust schools will:

- develop a strategic approach which enables online/remote learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school.

- when selecting online learning platforms (outside of those provided by the Trust) first consider data protection. Schools will complete a privacy impact assessment (DPIA) and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely. DPIA's will be shared with the Trust ICT team and approved before procurement of such systems.
- consult with the Trust ICT manager to prevent duplication of services where such services exist within Trust provided systems.
- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given
- make sure that administrative access to platforms is recorded in the privileged access log
- make sure that administrative access to platforms will be multi factor and password protected and run with approval from the School's Senior Leadership Team. The Trust ICT team will report any systems not recorded in the privileged access log to School and Trust leadership.
- ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content.
- discuss the use of online/remote learning as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice, being careful about subjects discussed online.
- register concerns (e.g. recording in Online Safety log) regarding pupils' inappropriate use (in or out of school) and raise with their parents and carers.
- support staff to deal with the consequences of hurtful or defamatory posts about them online.

With respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing

Trust schools will:

- restrict access to social media and social networking sites in school to staff (access to Youtube for Schools may be requested from the Trust ICT team for pupils)
- adhere to the Trust's process for social media setup to support staff who wish to use social media in the classroom to run a class blog/Twitter/YouTube account to share learning experiences.
- provide staff with understanding of UK GDPR to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given.
- make sure that staff official blogs or wikis will be password protected and run with approval from the Senior Leadership Team
- ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content in line with the Trust's social media policy.
- discuss with staff the personal use of email, online learning platforms, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice, being careful about subjects discussed online.
- staff are advised that no reference should be made to pupils, parents/carers or school staff on their personal social networking accounts.

- register concerns (e.g. recording in Online Safety log) regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites.
- support staff to deal with the consequences of hurtful or defamatory posts about them online.
- inform the staff that in the case of a Critical Incident they should not make any comment on social media without the permission of the senior management team.

With respect to personal devices (including consideration of Keeping Children Safe 2023)

Trust schools will:

- inform staff that personal devices should only be used at break and lunchtimes in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher (turned off at other times).
- ensure that staff understand that the Trust Staff and Volunteers AUP will apply to the use of their own portable / wearable device for school purposes.
- inform staff and visitors that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Trust or School SLT. School SLT school should confirm permission for each school event where it is reasonable for parents to take photos and video of their child during performances.
- check any use of a personal device for an education purpose (where permission has been given) only uses the school's guest internet connection on the school site.
- remind all that personal devices should be pin code or fingerprint protected and not discoverable by third parties (the Trusts ICT Security policy details requirements for devices to connect to school services).
- advise staff not to use their personal mobile phone to contact pupils, parents and carers
- provide a mobile phone/tablet to staff for activities that require them on a regular basis.
- challenge staff and visitors when there is suspected misuse of mobile phones or devices.
- when pupils are allowed personal devices in school, they are used within the school's behaviour policy / code of conduct, and pupils understand they can be asked to account for their use.
- use the right to collect and examine any pupil device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school internet connection.

The following table shows how Trust schools consider the way these methods of communication should be used.

Communication Technology	Staff and other Adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff*	Not allowed	Allowed	Allowed at certain times	Allowed for selected pupils	Not allowed
Mobile Phones/Wearable Technology	X							X
Use of personal mobile phones/wearable technology in lessons				X				X
Use of mobile phones/wearable technology in social time	X							X
Taking photos on personal mobile phones or other camera devices			X					X
Taking photos on school owned mobile phones or other camera devices		X						X
Use of personal devices including wearable technology		X						X
Use of 'always on' voice activated technology			X				X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X				X
Use of chat facilities, forums and closed groups in apps		X						X
Use of messaging apps		X						X
Use of social networking sites for school business			X					X
Use of social networking sites for personal use		X						
Use of blogs for school business			X					X
Use of blogs for personal use		X						
Use of public messaging apps e.g Twitter/X/Threads for school business			X					X
Use of public messaging apps e.g Twitter/X/Threads for personal use		X						
Use of video broadcasting e.g. YouTube			X					X
Use of video broadcasting e.g. YouTube for personal use		X						
Use of live video streaming e.g. Microsoft Teams, Zoom for learning/professional use	X					X		

* Selected staff should seek authorisation from the Headteacher before using personal equipment/school social media. Staff with access to School social media accounts should be referenced in the privileged access log.

Sanctions and Disciplinary Proceedings

Sanctions and disciplinary procedures may be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation):

- child sexual abuse images.
- grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content.
- promotion of any kind of discrimination, racial or religious hatred.
- personal gambling or betting.
- any site engaging in or encouraging illegal activity including radicalisation and terrorism.
- threatening behaviour, including promotion of physical violence or mental harm.
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school or organisation into disrepute.
- using Trust or school systems to run a private business.
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust and its schools.
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords).
- creating or propagating computer viruses or other harmful files.
- carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet.

The 2011 Education Act increased powers with regard to pupils and the searching for and of electronic devices and the deletion of data. These are applied through the school's Behaviour Policy.

All incidents will have unique context and require different sanctions. For pupils, these should be considered at school level Appendix A will be filled in by each school in line with the school's behaviour policy.

Schools should follow the Trust's code of conduct, child protection and/or disciplinary policies with advice from the Trust HR Team.

Appendix A: Action to take in response to inappropriate use

Schools should use the grid below marking appropriate action to incidents relating to Pupils

Incidents will have unique contexts and may need different levels of response especially in relation to their type and severity. Therefore, ticks may appear in more than one column.

The ticks in place are actions which must be followed.

Incident Type	Refer to class teacher / tutor	Refer to Headteacher	Refer to LADO	Refer to Police	Refer to Trust ICT staff for action re filtering / security etc	Inform parents / carers	Removal of network /internet access rights	Warning	Further sanction e.g., exclusion
Deliberately producing, accessing, or trying to access, material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✖	✖	✖	✖	✖	✖	✖	✖	
Unauthorised use of non-educational sites during lessons	✖	✖			✖	✖	✖	✖	
Unauthorised use of mobile phone / wearable technology / personal tablet	✖	✖			✖	✖	✖	✖	
Unauthorised use of social networking / instant messaging / personal email	✖	✖			✖	✖	✖	✖	
Unauthorised downloading or uploading of files	✖	✖			✖	✖	✖		
Allowing others to access school network by sharing username and passwords	✖	✖			✖	✖	✖	✖	
Attempting to access or accessing the school network, using another pupil's account	✖	✖			✖	✖	✖	✖	
Attempting to access or accessing the school network, using the account of a member of staff	✖	✖			✖	✖	✖	✖	
Corrupting or destroying the data of other users	✖	✖		✖	✖	✖	✖	✖	
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature	✖	✖	✖	✖	✖	✖	✖	✖	
Continued infringements of the above, following previous warnings or sanctions									✖
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✖	✖	✖	✖	✖	✖	✖	✖	✖
Using proxy sites or other means to subvert the school's filtering system	✖	✖	✖		✖	✖	✖	✖	✖
Accidentally accessing offensive or pornographic material and failing to report the incident	✖	✖	✖		✖	✖	✖	✖	✖
Deliberately accessing or trying to access offensive, pornographic or extremist material	✖	✖	✖		✖	✖	✖	✖	✖
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✖	✖			✖	✖	✖	✖	✖

Appendix B: Information for Parents Template

Appropriate Filtering and Monitoring of Internet Access

The Trust provide all Trust schools with a platform to appropriately filter and monitor Internet access based upon age and role within the school.

Recognising that no filter can guarantee to be 100% effective, the Trust and its schools are satisfied that their filtering system manages the following content (and web search).

Content	Note
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
Drugs & Substance Abuse	Displays or promotes the illegal use of drugs or substances
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance
Malware/Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	Displays sexual acts or explicit images
Piracy and copyright Theft	Includes illegal provision of copyrighted material
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)
Violence	Displays or promotes the use of physical force intended to hurt or kill
Illegal activity	IWF Filter lists for Child Sexual Abuse Material & the Home Office Police assessed list of unlawful terrorist content

This list is not exhaustive and in addition, Schools may choose to filter and block any Internet content where it impedes or is detrimental to Teaching and Learning.

The Trust retain logs of Internet access of all pupils for 12 months. School staff regularly review blocked content and are alerted to attempts to access information in blocked categories. The school's designated safeguarding lead investigates and can provide more information on monitoring processes within school.

Please note that all school owned devices (including any SEN provisioned devices treated as part of the schools IT estate) will filter internet access on any internet connection and are therefore monitored.

Email Communication and Monitoring

All pupils are provisioned with an email account as they are technically integral to the functionality of Teams and other systems that are used within the School and Trust.

Our Trust ICT Team ensure:

- Emails to pupil accounts can only be received from staff and pupils within the School.
- Governors cannot send emails to pupils.
- Pupils cannot see the email address of other staff and pupils within the Bath & Wells Multi Academy Trust.
- All email from and destined to external sources is blocked by default. Schools may choose to allow email to and from specific destinations (such as other schools).

A list of external organisations that the school allows pupil communication with can be obtained from the school on request.

Teams and Learning Platform Communication Monitoring

All pupils may use Microsoft Teams, Google Classroom and Apple Class as part of the School curriculum.

The Trust ICT Team ensure that pupils cannot instigate communication privately within these services either by instant message or video chat.

Online Video/Audio meetings end automatically when a staff member is no longer present.

Other platforms and content used by our school

Content/Platform	What do we use it for?
EXAMPLE: Numbots	Math practice for KS2

Privacy

All systems used within the school are owned and managed by the Bath & Wells Multi Academy Trust.

Pupils and Parents should have expectation of privacy whilst using such systems. The Trust or school may investigate any Online Safety incident and access any pupil's mailbox/OneDrive/other Trust system without parental permission. Such investigations and any actions are fully audited.

Appendix C: Methods of Communication for display

This table shows how Trust Schools consider ways of communication and when/how they should be used.

Communication Technology	Staff and other Adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff*	Not allowed	Allowed	Allowed at certain times	Allowed for selected pupils	Not allowed
Mobile Phones/Wearable Technology	X							X
Use of personal mobile phones/wearable technology in lessons				X				X
Use of mobile phones/wearable technology in social time	X							X
Taking photos on personal mobile phones or other camera devices			X					X
Taking photos on school owned mobile phones or other camera devices		X						X
Use of personal devices including wearable technology		X						X
Use of 'always on' voice activated technology			X				X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X				X
Use of chat facilities, forums and closed groups in apps		X						X
Use of messaging apps		X						X
Use of social networking sites for school business			X					X
Use of social networking sites for personal use		X						
Use of blogs for school business			X					X
Use of blogs for personal use		X						
Use of public messaging apps e.g Twitter/X/Threads for school business			X					X
Use of public messaging apps e.g Twitter/X/Threads for personal use		X						
Use of video broadcasting e.g. YouTube			X					X
Use of video broadcasting e.g. YouTube for personal use		X						
Use of live video streaming e.g. Microsoft Teams, Zoom for learning/professional use	X					X		

* Selected staff should seek authorisation from the Headteacher before using personal equipment/school social media. Staff with access to School social media accounts should be referenced in the privileged access log.