Online Safety Policy

Version	Date	Author	Changes
V1	March 2020	A&R	Approved policy
V2	2/3/21	GLy	Addition of policies and other guidance. Included the statutory RSE guidance (with particular reference to the online content). Updated resources in Appendix C.
V3	8/3/21	RM	Section 6.1 allowance for use of mobile phones for work purposes
V4	12/5/21	TH	Updates to Review Period and Consultation Pathway
V5.2	10/05/23	GLy	Review as per timescale, update to terminology
V6	30/10/24	TD	Section 3.10 – Whole School Approach – additional information included covering what children will be directly taught. Section 3.11 – Requirements for DSLs and Staff to evidence training and understanding of the filtering and monitoring system. 4.3 – Reference to filtering and monitoring training. 4.3 – Filtering and monitoring considerations for vulnerable pupils including those with SEND. Update to consultation pathway (Job titles updated) Removed word disciplinary from the AUP and replaced it with 'sanctions inline with the behaviour policy. Updated Lead Professional for the Policy Removed reference to schools modifying AUP for mobile phone use and included to read inline with the Futura IT policy.

Lead professional: Trust Inclusion and Safeguarding Lead
Adopted: June 2021
Review timescale: 2 years
Consultation path:
Trust Lead for Inclusion and Safeguarding Head of IT Service
CEO
ELG
Audit and Risk Committee
Trade union approval: N/A
Next review: November 2025

Online Safety Policy

Contents

1. Aims and Scope 4

2.0 Policies and Practices 5

2.1 Writing and reviewing the Online Safety Policy 5

2.2 Online Safety Monitoring 6

2.3 Key responsibilities for the community 8

2.4 Authorising internet access 11

2.5 Responding to Online Incidents and Safeguarding Concerns (Summary - Appendix A) 12

2.6 Online Communication and Safer Use of Technology 13

Managing the school website 13

2.7 Publishing images and videos online 13

2.8 Managing email 13

2.9 Official videoconferencing and webcam use for educational purposes 14

2.10 Users 14

2.11 Content 14

2.12 Managing personal data online 15

3.0 Education and Training 15

3.1 Teaching and learning 15

3.2 Online Safety for vulnerable pupils, including those with special educational needs 16

3.3 Engagement Approaches 16

3.4 Underpinning knowledge and behaviours 16

3.5 Harms and risks 16
3.6 How to stay safe online 17
3.7 Wellbeing 17
3.8 Relationships Education, Relationships and Sex Education (RSE) and Health Education 17
3.9 Teaching about online harms and risks in a safe way 18
3.10 Whole school approach 18
3.11 Including engagement and education of staff 19
3.12 Engagement and education of parents and carers 19
4.0 Infrastructure and Technology 20
4.1 Security and Management of Information Systems 20
4.2 Password policy 20
4.3 Filtering and Monitoring 20
4.4 Management of applications (apps) used to record children's progress 21
5.0 Social Media Policy 21
5.1 General social media use 21
5.2 Official use of social media 22
5.3 Staff personal use of social media 23
5.4 Staff official use of social media 23
5.5 Pupils' use of social media 24
6.0 Use of Personal Devices and Mobile Phones 25
6.1 Rationale regarding personal devices and mobile phones 25
6.2 Expectations for safe use of personal devices and mobile phones 25
6.3 Pupils' use of personal devices and mobile phones 25
6.4 Staff use of personal devices and mobile phones 26
6.5 Visitors use of personal devices and mobile phones 26
Appendix A: 27
Appendix B 28
Responding to concerns regarding radicalisation and extremism online 28
Appendix C 28
Appendix D – Staff Acceptable Use Policy 30
Appendix E – Pupil Acceptable Use Policy 32

1. Aims and Scope

Futura Learning Partnership ('the trust') believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

The trust identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

The trust has a duty to provide the community with quality internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

The purpose of the trust Online Safety Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that each school is a safe and secure environment.
- Safeguard and protect all members of each schools' communities online
- Raise awareness with all members of each schools' communities regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

Each school's Online Safety Policy (trust Online Safety Policy) applies to all staff including the Local Governance Committee, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school or trust (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.

The policy applies to all access to the internet and use of information communication devices, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop, tablet or mobile phone.

Mr Gary Schlick , Futura Learning Partnership

2.0 Policies and Practices

2.1 Writing and reviewing the Online Safety Policy

The Online Safety Policy is reviewed biennially and should be read in conjunction with other relevant trust and school policies:

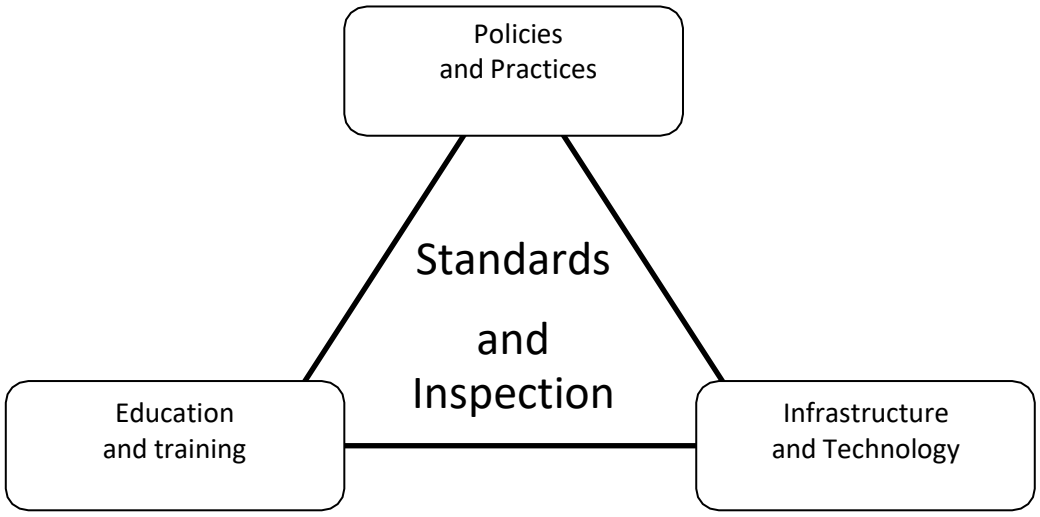
- Trust Child Protection and Safeguarding Policy
- *Mary Elton Primary School* Behaviour for Learning Policy
- *Mary Elton Primary School* Anti-bullying Policy
- *Mary Elton Primary School* PSHE Policy
- Relationship and Sex Education Policy
- *Mary Elton Primary School* Home School Agreement
- Safeguarding Concerns and Allegations Against Staff Policy
- Staff Safer Working Policy
- IT Security Policy

All action is taken in line with the following legislation/guidance:

- South West Child Protection Procedures (SWCPP)
- The Children Act 1989 and 2004
- The Children and Families Act 2014
- The Serious Crime Act 2015
- The Sex Offenders Act 2003
- Section 175 Education Act 2002
- The Education (Health Standards) (England) Regulations 2003
- The Education (Pupil Referral Units) (Application of Enactments) (England) Regulations 2007 as amended by SI 2010/1919, SI 2012/1201, SI 2012/1825, SI 2012/3158
- The School Staffing (England) Regulations 2009 as amended by SI 2012/1740 and SI 2013/1940
- The Education (Non-Maintained Special Schools) (England) Regulations 2011 as amended by SI 2015/387
- The Education (School Teachers' Appraisal) (England) Regulations 2012
- Computer Misuse Act 1990
- General Data Protection Regulation 2018
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Copyright Design and Patents Act 1988
- Telecommunications Act 1984
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Criminal Justice and Immigration Act 2008
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964
- Human Rights Act 1998
- The Equality Act 2010

- The Education and Inspections Act 2006 and 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- The Counter Terrorism and Security Act 2015
- Keeping Children Safe in Education 2024
- Working Together to Safeguard Children 2018
- Safeguarding Children and Safer Recruitment in Education 2007
- Local Safeguarding Children Board Guidance
- Guidance for Safer Working Practices 2018
- The Prevent duty – Advice for schools and childcare providers 2015
- What to do if you're worried a child is being abused 2015
- Teaching online safety in schools 2019
- Sharing nudes and semi-nudes: advice for education settings working with children and young people 2020
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (2019)

The trust recommends the use of the Becta PIES model which offers an effective strategic framework for approaching online safety. This model illustrates how a combination of effective policies and practices, education and training, infrastructure and technology underpinned by standards and inspection can be an effective approach to manage and limit online safety risks.



Becta 2008 – Safeguarding Children in a Digital World

2.2 Online Safety Monitoring

This self-audit has been completed by the member of the **MARY ELTON PRIMARY SCHOOL** Senior Leadership Team (SLT) responsible for Online Safety. The title for this role is Online Safety Coordinator (OSC). Staff that have contributed to the audit include: Designated Safeguarding Lead, Director of Inclusion, ICT (Curriculum Lead – Online Safety), Head of IT Services and the Headteacher.

Issue	Action	Notes

Has the trust an online safety policy that complies with available guidance?	Yes	
Date of latest update	November 2024	
The trust Online Safety Policy was adopted by governors on	January 2025	
The policy is available for staff at www.maryeltonschool.org.uk	Yes	
The policy is available for parents/carers at www.maryeltonschool.org.uk	Yes	
The responsible member of the School Leadership Team is	**Tom Newell**	
The governor responsible for Online Safety is	**Hadley Rides**	
The Designated Safeguarding Lead (DSL) is	**Tom Newell**	
The Online Safety Coordinator (OSC) is	**Cheryl Brown / Tom Newell**	
The Prevent Single Point of Contact (PSOC) is	**Tom Newell**	
Is there a clear procedure for a response to an incident of concern?	Yes	See Appendix A
Have online safety materials from CEOP been obtained?	Yes	On school website
Staff are made aware of the school's Acceptable Use Policy.	Yes	**MARY ELTON PRIMARY SCHOOL** Staff Acceptable Use Policy – Appendix D
Pupils are made aware of the school's Acceptable Use Policy.	Yes	**MARY ELTON PRIMARY SCHOOL** Pupil Acceptable Use Policy – Appendix E
Are all pupils aware of the school's online safety and receive education on online safety?	Yes	e.g. IT Education, assemblies and PSHE
Do pupils know how to report concerns that they might have?	Yes	
Do parents/carers sign and return an agreement that their child will comply with the school online safety rules?	Yes	
Are staff, pupils, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced?	Yes	Mentioned in welcome sheet given to visitors.
Personal data is collected, stored and used according to the principles of the Data Protection Act	Yes	
Internet access is provided by an approved educational Internet service provider which complies with DfE requirements.	Yes	
School-level filtering has been designed to reflect educational objectives and approved by the SLT?	Yes	
Staff with responsibility for managing, filtering, network access and monitoring are adequately supervised by a member of SLT?	Yes	Mr R May
Appropriate teaching and/or technical members of staff have attended training on filtering systems?	Yes	IT Services Team
Are staff made aware of online safety issues and know how to deal with them?	Yes	Through this and other policies and training.

		PSHE curriculum. Computing curriculum/training. Safer internet day.
Do staff know how to conduct themselves professionally online?	Yes	Through the trust Staff Code of Conduct and MARY ELTON PRIMARY SCHOOL Online Safety Policy. Annual staff training and induction online safety training
Are parents/carers given the opportunity to be educated to keep their children safe online?	Yes	Through a variety of sources such as CEOP and B&NES.
The Local Governance Committee will receive a report on the implementation of the online policy (which will include anonymous details of online safety incidents) at regular intervals.	Yes	LGC annually as part of Child Protection Report.
The Online Safety Policy will be reviewed bi-annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	June 2026	

2.3 Key responsibilities for the community

The key responsibilities of each school's SLT are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue
- Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring that there are appropriate up-to-date policies and procedures regarding online safety including an Acceptable Use Policy (the school's AUP), which covers appropriate professional conduct and use of technology.
- Ensuring the AUP is read and signed by all staff on joining the school/trust.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect pupils from inappropriate content that meet the needs of the school community, whilst ensuring pupils have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks, and to ensure that the school network system is monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities, and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum that enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.

- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the trust to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of each Local Governance Committee (LGC) is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

The key responsibilities of the DSL (SLT i/c Online Safety) at each school are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- To report to the school's SLT, Local Governance Committee and other agencies as appropriate, on online safety concerns and local data/figures.
- Meet regularly with the governor with a lead responsibility for online safety.
- Working with the school's SLT to review and update the Online Safety Policy, the school's AUP and other related policies on a regular basis (at least annually) with stakeholder input.
- Work with the trust lead for data protection and data security to ensure that practice is in line with current legislation.
- Co-ordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Ensuring training and advice for staff is in place.
- Monitor the school online safety incidents to identify gaps/trends and use this data to update the school's education response to reflect need.
- Ensuring an online safety group is in place that includes input from all stakeholder groups.

The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school's AUP and trust Staff Code of Conduct and adhering to them. This should be completed when a member of staff joins the trust. All staff should sign to confirm this has been completed.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.

- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery wherever possible.
- Ensuring pupils understand and follow the Online Safety Policy and the school's AUP.
- Developing pupils' understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Monitoring ICT activity in lessons, extra-curricular and extended school activities.
- Reporting any individuals of concern, suspected misuse or problems to the DSL for investigation.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on- and off-site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with each school's SLT.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated as necessary and that responsibility for its implementation is shared with the line manager and DSL.
- Ensuring that the use of each school's network is monitored and is reporting any deliberate or accidental misuse to the Headteacher and DSL.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- In conjunction with the line manager and DSL, report any breaches and liaise with local or national bodies as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and each school's SLT, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's IT infrastructure/system is secure and not open to misuse or malicious attack. Please see the IT Security Policy for more details.

The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school's AUP and adhering to it.
- Respecting the feelings and rights of others both online and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Having a good understanding of research skills, and the need to avoid plagiarism and uphold copyright regulations.

- Needing to understand the importance of reporting abuse, misuse or access to inappropriate materials, and know how to do so.
- Knowing and understanding school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on online bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Online Safety Policy covers their actions out of school, if related to their membership of the school.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

The key responsibilities of parents and carers are:

- Reading the school's AUP, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school's online safety policies.
- Using school systems safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Community Users

- Community Users who access school IT systems as part of the extended school provision will be expected to sign the school's AUP before being provided with access to school systems.

2.4 Authorising internet access

- Each school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the school's AUP before using any school resources.
- Parents will be informed that pupils will be provided with supervised internet access that is appropriate to their age and ability.
- Parents will be asked to read the school's AUP for pupil access and discuss it with their child, where appropriate.
- Parents or carers of all pupils are given the opportunity to opt out of internet access.

- When considering access for vulnerable members of the community (such as with pupils with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- Pupil or staff access to the internet can be withdrawn should it be deemed necessary by the relevant member of SLT.

2.5 Responding to Online Incidents and Safeguarding Concerns (Summary - Appendix A)

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sharing nudes, online/cyber bullying, etc. This will be highlighted annually within staff training and educational approaches for pupils.
- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sharing nudes, cyberbullying, illegal content, etc.
- The DSL will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the North Somerset thresholds and procedures.
- Complaints about internet misuse will be dealt with under the school's Complaints Procedure
- Complaints about online/cyber bullying will be dealt with under the school's Anti-Bullying Policy and procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's Complaints Procedure.
- Staff will be informed of the Complaints and Whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the MARY ELTON PRIMARY SCHOOL Behaviour for Learning Policy, where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as 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 Police via 101, or 999 if there is immediate danger or risk of harm.
- 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 the police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to North Somerset.
- Parents and children will need to work in partnership with the school to resolve issues.

2.6 Online Communication and Safer Use of Technology

Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number.
- Staff or pupils' individual contact details will not be published.
- The Headteacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Parents or carers can state that their child's work should not be published on the school website or other online space. Parents will be reminded of this annually via the school newsletter.
- The administrator account for the school's website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

2.7 Publishing images and videos online

- Parents or carers must give specific permission for the use of images/video including their child before they can be published on the school website or other online space.
- No pupil will be identified in an image/video on the school website or other public online space without parental or carer consent.

2.8 Managing email

- Pupils may only use school provided email accounts for educational purposes.
- All members of staff are provided with a specific work email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and may be reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent in an encrypted attachment.
- Access to the school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- Members of the community must immediately tell the OSC if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work-life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Excessive social email use can interfere with teaching and learning, and will be restricted. Access in school to external personal email accounts may be blocked.
- Emails sent to external organisations should be written carefully and authorised before sending if appropriate- in the same way as a letter written on school headed paper would be.

- School email addresses and other official contact details should not be used for setting up personal social media accounts.

2.9 Official videoconferencing and webcam use for educational purposes

- The school acknowledges that video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- All video conferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- Video conferencing contact details and external IP addresses will not be posted publicly
- Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
- School video conferencing equipment will not be taken off school premises without permission.
- Staff will ensure that external video conference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

2.10 Users

- Pupils will ask permission from a teacher before making or answering a video conference call or message.
- Video conferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers' consent will be obtained prior to pupils taking part in video conferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to video conferencing administration areas or remote control pages.
- Unique log on and password details for the educational video conferencing services will only be issued to members of staff and kept secure.

2.11 Content

- When recording a video conference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a video conference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

2.12 Managing personal data online

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Please consult the Data Protection Policy for details of how the trust complies with this requirement.

3.0 Education and Training

3.1 Teaching and learning

Appropriate and safe classroom use of the internet and any associated devices.

- Internet use is a key feature of educational access and all pupils will receive age- and ability-appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- The school's internet access will be designed to enhance and extend education.
- All members of staff are aware that they cannot rely on filtering alone to safeguard pupils and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their ability and understanding.
- All school-owned devices will be used in accordance with the school's AUP 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.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age-appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of the community.
- The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- The School will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3.2 Online Safety for vulnerable pupils, including those with special educational needs

All trust schools are aware that there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Schools will consider how they tailor their offer to ensure these pupils receive the information and support they need.

3.3 Engagement Approaches

Engagement and education of children and young people

3.4 Underpinning knowledge and behaviours

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. Trust schools will focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.

Underpinning knowledge and behaviours include:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- How and when to seek support

3.5 Harms and risks

Trust schools will have an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their pupils.

The topics below have been taken from the Department for Education document 'Teaching Online Safety, 2019'. In this document there is signposting to the Education for a Connected World Framework(https://www.gov.uk/government/publications/education-for-a-connected-world), which includes age-specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives, including how to navigate online safely. This was developed by the UK Council for Internet Safety.

Trust schools will cover a range of topics linked to individual harms and risks. These may include:

- Age restrictions
- Content: How it can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam email
- Fraud (online)
- Password phishing
- Personal data
- Persuasive design
- Privacy settings
- Targeting of online content including on social media and search engines.

3.6 How to stay safe online

Trust schools will cover a range of topics linked to a pupil's personal safety or the personal safety of others online. These may include:

- Abuse (online)
- Challenges
- Content which incites
- Fake profiles
- Grooming
- Live streaming
- Pornography
- Unsafe communication

3.7 Wellbeing

Trust schools will cover a range of topics linked to how online activity can adversely affect a pupil's wellbeing. These may include:

- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health and relationships
- Online vs. offline behaviours
- Reputational damage
- Suicide, self-harm and eating disorders.

3.8 Relationships Education, Relationships and Sex Education (RSE) and Health Education

Trust schools will adhere to the Government guidance *Relationships Education, Relationships and Sex Education (RSE) and Health Education* (2020). The content contained within this document will form part of the school's curriculum, including the ICT and PSHE curricula. By the end of each stage in a pupil's education, they must have been taught particular concepts.

By the end of primary school, all pupils should 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.

By the end of secondary school, all pupils should 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.

3.9 Teaching about online harms and risks in a safe way

As with the potential that a child (or more than one child) in the class may be suffering from online abuse or harm in this way, it is important to create a safe environment in which pupils feel comfortable to say what they feel. For example, during lessons a pupil should not feel that they will get into trouble and/or be judged for talking about something which happened to them When starting a lesson, teachers should establish a class 'code of conduct', creating a culture on confidentiality and support.

Where schools are already aware of a child who is being abused or harmed online they should carefully plan any lesson to consider this.

In some cases, a pupil will want to make a disclosure following a lesson or activity. The lesson may have provided the knowledge that enabled the pupils to realise they are being abused or harmed and/or give them the confidence to say something. All trust schools regularly promote to pupils what the school's reporting mechanisms are. As per "Keeping Children Safe in Education" those mechanisms should be child friendly and operate with the best interests of the pupil at their heart.

3.10 Whole school approach

All trust schools will adopt whole-school approaches to teaching about online safety that goes beyond classroom teaching to include all aspects of school life, including culture, ethos, environment and partnerships with families and the community.

Our effective whole school approach to online safety is to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Pupils will be taught about the breadth of issues classified within online safety that can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; 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: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group

3.11 Including engagement and education of staff

- DSLs will evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
- All staff (including governors and trustees) will receive appropriate safeguarding and child protection training, including online safety at induction. This will include, amongst other things, an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- The Online Safety (e-Safety) Policy will be formally provided to and discussed with all members of staff as part of induction and will be annually reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training on safe and responsible internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- The Head of IT Service receives regular training to ensure the trust Online Safety Policy is compliant with national and local guidance.

3.12 Engagement and education of parents and carers

- Each school recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school Online safety (e-Safety) Policy and expectations in newsletters, letters, the school's prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school's AUP for pupils and discuss its implications with their children.

- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

4.0 Infrastructure and Technology

4.1 Security and Management of Information Systems

- The Head of IT Services will be responsible for ensuring that all school networks are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Please see the IT Security Policy for details regarding this.

4.2 Password policy

- All data is protected by an appropriate level of security such as a password, PIN or other method of authentication. Please see the IT Security Policy for more details.

4.3 Filtering and Monitoring

- The Head of IT Services will ensure that the school has age- and ability-appropriate filtering and monitoring in place whilst using school devices and systems to limit pupils' exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of its community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- Filtering and monitoring decisions consider those who are potentially at greater risk of harm for examples pupils with SEND, and how often they access the IT system.
- All monitoring of school-owned/provided systems will take place to safeguard members of the community.
- All staff (including governors and Trustees) will receive appropriate safeguarding and child protection training, including online safety at induction. This will include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- 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.
- The school uses educational filtered secure broadband connectivity that is appropriate to the age and requirement of our pupils.
- The school will ensure that the filtering policy is regularly reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to IT Services and will then be recorded and escalated as appropriate.
- The school will use a web content filtering product which will as a minimum:
  - Subscribe to the Internet Watch Foundation Child Abuse Images and Content (CAIC) URL List;
  - Block all illegal material identified by the Internet Watch Foundation (IWF);
  - Capable of blocking the vast majority of inappropriate content in each of the following categories:
    - Pornographic, adult, tasteless or offensive material;
    - Violence (including weapons and bombs);

    - Racist, extremist, radicalisation and hate material;
    - Illegal drug taking and promotion;
    - Criminal skills and software piracy.
- Changes to the school filtering policy will be risk assessed by the Head of IT Services prior to any changes and where appropriate with consent from the Leadership Team. All changes to the school filtering policy will be logged.
- The SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies.

4.4 Management of applications (apps) used to record children's progress

- The Headteacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems that store personal data will be risk assessed prior to use. Please see the Data Protection Policy for details regarding this.
- Only school-/setting-issued devices will be used for apps that record and store children's personal details, attainment or photographs locally on the device.
- Devices will be appropriately encrypted if taken off-site to prevent a data security breach in the event of loss or theft. Please see the IT Security Policy for details regarding this.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the school's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

5.0 Social Media Policy

5.1 General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the trust community and exist in order to safeguard both the school and the wider community, online and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the trust community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the trust community.
- All members of the trust community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Each school will control pupil and staff access to social media and social networking sites whilst on-site and when using school provided devices and systems. The use of social networking applications during school hours for personal use is not permitted by staff and pupils.
- Any concerns regarding the online conduct of any member of the trust community on social media sites should be reported to the OSC or Headteacher (staff concerns) and will be managed in accordance with policies such as the Anti-Bullying Policy, Staff Code of Conduct,

Safeguarding Concerns and Allegations Against Staff Policy, Behaviour Policy and the Child Protection and Safeguarding Policy.

- Candidates shortlisted for interview will be advised that online searches will be done as part of due diligence.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as the Anti-Bullying Policy, Staff Code of Conduct, Safeguarding Concerns and Allegations Against Staff Policy, Behaviour Policy and the Child Protection and Safeguarding Policy.

5.2 Official use of social media

- The trust and individual schools have established official social media channels.
- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher.
- Members of staff running official social media channels will sign a specific school's AUP to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including the Anti-Bullying Policy and the Child Protection and Safeguarding Policy.
- Images or videos of children will only be shared on official social media sites in accordance with the advice in this policy and where the appropriate consents have been received.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, be linked to from the school website and take place with written approval from the SLT.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Public communications on behalf of the school will, where possible, be read and agreed by the Headteacher or a nominated deputy.
- Official social media channels will link back to the school website and/or the school's AUP to demonstrate that the account is official.
- The school will ensure that any official social media use does not exclude members of the community who are unable to use social media channels.

5.3 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school's AUP.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.
- Staff will discuss the circumstances with the Headteacher if ongoing contact with pupils is required once they have left the school roll.
- All communication between staff and members of the school community on school business will take place via official approved communication channels.
- Any communication from pupils received on personal social media accounts will be reported to the school's DSL.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues, etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools' policies and the wider professional and legal framework.
- Members of staff will notify the OSC immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- Members of staff are encouraged not to identify themselves as employees of the trust on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- Trust email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the school's social media channels will be advised to use dedicated professionals' accounts, where possible, to avoid blurring professional boundaries.

5.4 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the trust, then they are requested to be professional at all times and to be aware that they are an ambassador for their school and the wider trust community.

- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel complies with the school's policies in relation to written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so by the Headteacher or delegated deputy.
- Staff using social media officially will inform their line manager, the DSL and/or the Headteacher or Chief Operating Officer of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with pupils or parents/carers through social media and will direct them to communicate via official communication channels.
- Staff using social media officially will sign the school's AUP.

5.5 Pupils' use of social media

- Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school's AUP.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age-appropriate sites that have been risk assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites that may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs, etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and secure passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for pupils under the age of 13, therefore the school will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including the Anti-Bullying Policy and Behaviour Policy.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

6.0 Use of Personal Devices and Mobile Phones

6.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among pupils and adults will require all members of the trust community to take steps to ensure that mobile phones and personal devices are used responsibly within and outside of school.
- The use of mobile phones and other personal devices by pupils and adults within school will be decided by each school with due allowance that the use of mobile phones by some staff is a necessary part of their work (for example Estates and IT Services) and is covered in appropriate policies including the Mobile Phone Policy.

6.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- Electronic devices of all kinds that are brought in on-site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Behaviour for Learning Policy and Anti-Bullying Policy.
- Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required.
- All members of the trust community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the trust community will be advised to use passwords/PINs to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and PINs should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the trust community will be 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 the school's policies.
- School mobile phones and devices must always be used in accordance with the school's AUP.
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/PIN and must only be accessed and used by members of staff.

6.3 Pupils' use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by pupils will take place in accordance with the Mobile Phone and Electronic Device Policy.
- Pupils' personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during school hours. Please see the IT Security policy for more details.

- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone outside of lesson time.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones and personal devices must not be taken into examinations/tests. Pupils found in possession of a mobile phone or personal device during an exam/test will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination/test or all examinations/tests.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Anti-Bullying Policy, or could contain youth produced sexual imagery (sharing nudes). The phone or device may be searched by a member of the SLT. Searches of mobile phones or personal devices will only be carried out in accordance with the DfE guidance which can be found at the following link: https://www.gov.uk/government/publications/searching-screening-and-confiscation
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

6.4 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal contact details for contacting pupils and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with their line manager.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Bluetooth or other forms of communication on personal devices should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used by teaching staff during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content brought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches this policy, then disciplinary action may be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the trust Safeguarding Concerns and Allegations Against Staff Policy.

6.5 Visitors use of personal devices and mobile phones

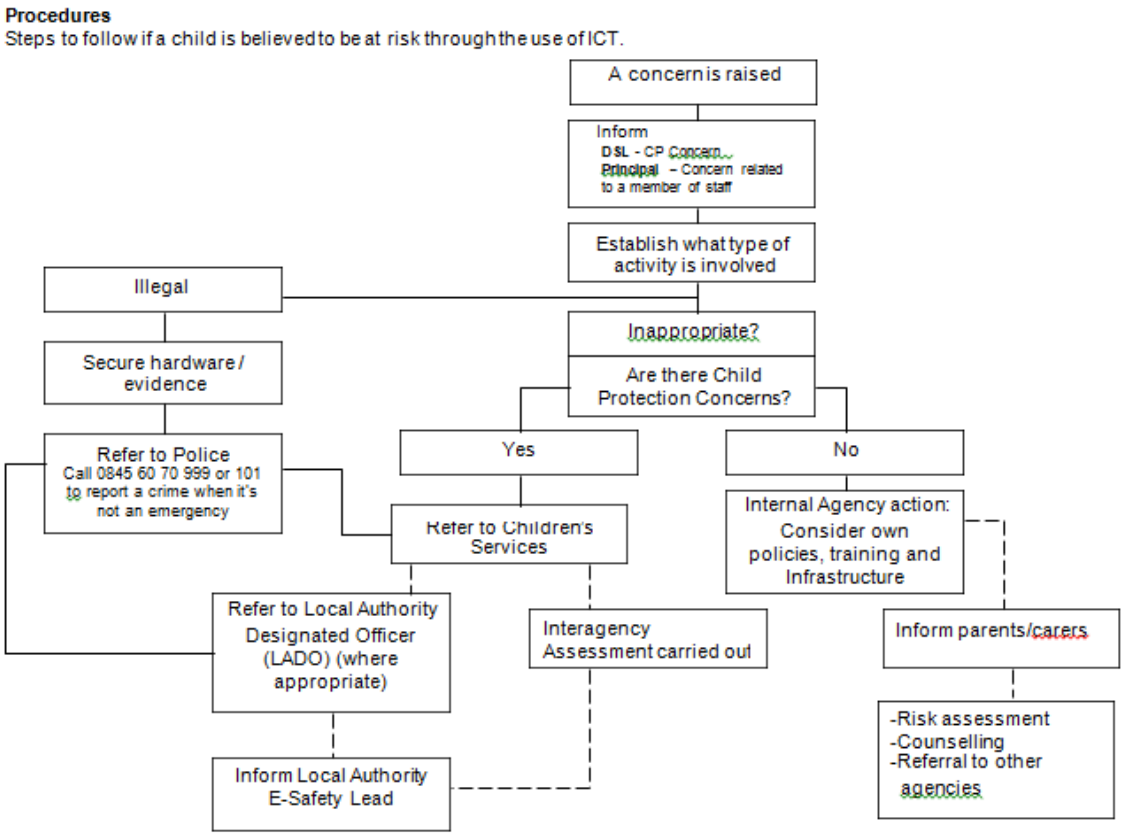
- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's Acceptable Use Policy.

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos is not allowed on school site. The Headteacher **may** allow parents/carers to take pictures or videos of their own children at special pupil performances, providing the pictures/videos **are not** shared on social media.

- Each school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

Appendix A:

Guidance on what to do if a concern is raised following an online safety incident:



Appendix B

Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. (Refer to item 4.3 filtering and monitoring.).
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the Child Protection and Safeguarding Policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including the Anti-Bullying Policy, Behaviour Policy, etc. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately via the LA Safeguarding Team and/or the Police.

Appendix C

Information & Organisations

CEOP - The Child Exploitation and Online Protection Centre is part of UK police and is dedicated to protecting children from sexual abuse wherever they may be. That means building intelligence around the risks, tracking and bringing offenders to account either directly or with local and international forces and working with children and parents to deliver our unique Think U Know educational programme. http://ceop.police.uk
Childnet International's mission is to work in partnership with others around the world to help make the Internet a great and safe place for children. Childnet works in 3 main areas of Access, Awareness, Protection & Policy. http://www.childnet.com
DfE - The Department for Education is responsible for education and children's services. http://www.education.gov.uk
IWF – The Internet Watch Foundation was established in 1996 by the UK internet industry to provide the UK internet 'Hotline' for the public and IT professionals to report potentially illegal online content within their remit and to be the 'notice and take-down' body for this content. IWF works in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of this content, specifically, child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to racial hatred content hosted in the UK. http://www.iwf.org.uk

Know IT All for Parents contains advice for parents and carers, and a special section for children and young people. http://www.childnet.com/kia/parents/
Local Safeguarding Children Board http://www.bathnes.gov.uk/services/children-young-people-and-families/child-protection/local-safeguarding-children-board
Report Abuse http://ceop.police.uk/safety-centre
UK Safer Internet Centre (UKSIC) - The UK Safer Internet Centre is co-funded by the European Commission and brought to you by a partnership of three leading organisations, Childnet International, the South West Grid for Learning and the Internet Watch Foundation. The UK Safer Internet Centre has three main functions: An Awareness Centre, a Helpline and a Hotline. http://www.saferinternet.org.uk
NSPCC – support for children, parents and staff regarding online safety: https://www.nspcc.org.uk/keeping-children-safe/online-safety/
Thinkuknow provides advice from the National Crime Agency (NCA) on staying safe online: https://www.thinkuknow.co.uk/
Parent Info is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations: https://parentinfo.org/
Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support: https://www.childnet.com/parents-and-carers/parent-and-carer-toolkit
Internet Matters provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world: https://www.internetmatters.org/?gclid=EAIaIQobChMIktuA5LWK2wIVRYXVCh2afg2aEAAYASAAEgIJ5vD_BwE
Let's Talk About It has advice for parents and carers to keep children safe from online radicalization: **https://www.ltai.info/staying-safe-online/**

UK Safer Internet Centre has tips, advice, guides and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services

https://www.saferinternet.org.uk/advice-centre/parents-and-carers

Appendix D – Staff Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the school's systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school's digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school's digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies.
- I will not try to upload, download or access any materials, which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based protected and restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the Police.

Appendix E – Pupil Acceptable Use Policy

ICT Acceptable Use Policy for Pupils

School laptops and iPads, School network access, internet use

Be Responsible

I will:

- ✓ Use electronic devices, the internet and the school network for educational purposes as directed by my teacher
- ✓ Use only my own accounts
- ✓ Securely log off at the end of each session

Be Respectful

I will:

- ✓ Communicate online in a respectful manner
- ✓ Treat school equipment with care
- ✓ Respect the work and privacy of others

Be Safe

I will:

- ✓ Keep my password and login information private
- ✓ Tell an adult if I read or see something on the internet that makes me feel uncomfortable
- ✓ Refrain from sharing any personal information on the internet

I understand that the use of technology is a privilege, not a right and inappropriate use will result in a cancelation of these privileges and may also include school sanctions in line with the behaviour policy if needed.