Pickwick Academy Trust

Online Safety Policy

(incorporating Acceptable Use)

Policy Group:	**Admin & Data**
Policy Ref:	**ADD/08**
Responsible Reviewing Officer and Job Title:	**Emma Oldale** **CFOO**
Date Written:	**September 2026**
Date Approved by the Board:	**October 2026**
Date of Next Review:	**September 2028**

1. Introduction

a. Pickwick Academy Trust recognises the great benefits that use of the internet brings to advance learning and development across the organisation, in particular for all pupils. We also recognise the threats that the internet contains and the harm that can be caused by others. This Online Safety Policy outlines the commitment of Pickwick Academy Trust to safeguard members of our school community online in accordance with statutory guidance and best practice.

b. This Online Safety Policy has been developed and reviewed by a group of users made up of:
   - *Trustees*
   - *Executive team members*
   - *Headteachers and members of the Senior Leadership team (including Designated Safeguarding Leads)*

2. Purpose and Scope

a. The Online Safety Policy is in place to:

   - set expectations for the safe and responsible use of digital technologies for learning, administration, and communication alongside a series of acceptable use agreements
   - allocate responsibilities for the delivery of the policy
   - provide up to date information, taking account of online safety incidents and changes/trends in technology and related behaviours
   - establish guidance for staff in how they should use digital technologies responsibly, in order to protect themselves and the school and how they should use this understanding to help safeguard pupils in the digital world
   - describe how the Trust and each school will help prepare pupils to be safe and responsible users of online technologies, especially those groups that are potentially at greater risk of online harm than others
   - establish clear procedures to enable the identification, reporting, response to and recording of the misuse of digital technologies and online safety incidents, including external support mechanisms

b. The 4 key categories of risk

   Our approach to online safety is based on addressing the following categories of risk, as determined by Keeping Children Safe in Education:

   - **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
   - **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or

young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

c. This Online Safety Policy applies to all members of the school community (including staff, pupils, trustees, governors, volunteers, parents and carers, visitors and contractors) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

d. The policy is made available at induction, on the staff shared drive and on the website of the trust and each school.

3. Responsibilities and Accountabilities

a. To ensure the online safeguarding of members of our trust community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

b. **The Trust Board is responsible for:**

- Ensuring the effectiveness of this policy by monitoring and reviewing it every year.
- Ensuring, through delegation to the CEO, Executive Team and Heads, and in conjunction with Local Governance Committees, the provision of adequate online safety provision, including filtering and monitoring systems and processes, across the Trust.
- Reviewing the information received from the School Improvement Committee on the level of online safety incidents across the trust alongside reviews of the filtering provision at each school. Online Safety Incident reports and the annual report on Filtering will be shared as part of the documentation provided to the Board by the School Improvement Committee.
- Ensuring that all members of the Board complete Annual Online Safety and Cyber Security training.
- Ensuring that all schools in the trust meet the DfE Cyber Security Standards.

c. **The CEO is responsible for**:

- Ensuring, through the Executive Team, that Headteachers and others associated with Online Safety are aware of the requirements of this policy and that the necessary arrangements are in place.

d. **The School Improvement Committee are responsible for:**

- Monitoring, through the receipt of collated and anonymised reports three times a year as part of the Headteachers report to the Director of Education the level of online safety incidents across the trust, alongside any additional information regarding trends or activities that have resulted higher levels of reporting and the actions put in place to address any areas of concern.
- Parents/carers are informed of patterns of online safety incidents as part of the school's raising of online safety awareness.
- Receiving answers to questions posed as part of the trust and Local Authority Safeguarding Audits, with reference to the UKCIS document "Online Safety in Schools and Colleges – questions from the governing body.
- Receiving an annual report on the review of the filtering provision at each school to ensure the trust is compliant with DfE Filtering and Monitoring Standards.
- Evaluating the impact of the Online Safety Policy and practice annually through review of the reports above.
- Ensuring that Online safety (and related) policies and procedures are updated annually in response to the evidence gathered from these reviews/audits/professional debate, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place.
- Ensuring that each school has an Online Safety Curriculum in place that is monitored by the Director of Education to ensure it meets the requirements of the National Curriculum.

e. **The Local Governance Committee is responsible for:**

- Reviewing the effectiveness of this policy in their school.
- Appointing a Governor to the role of 'Online Safety Governor', the responsibilities of which will include:
    - Regular meetings with the Designated Safeguarding Lead and Computing Lead.
    - Regularly receiving (collated and anonymised) reports of online safety incidents three times a year as part of the Headteachers report.
    - Checking that requirements outlined in the policy (*e.g. online safety education provision and staff training*) are taking place as required.
    - Ensuring that the filtering and monitoring provision is reviewed and recorded, at annually in line with the DfE Filtering and Monitoring Standards. This will form part of the Filtering and Monitoring Evaluation that is completed during consultancy meetings.
      (*The review will be undertaken by the SLT, the DSL, the IT provider and involve the Online Safety Governor and the Director of Education for the school)*
    - Reporting to the Local Governance Committee.
    - Receiving annual basic cyber-security training.
- Supporting the school by encouraging parents/carers and the wider community to become engaged in online safety activities.

f. **The CFOO**

- Retains accountability for Information Security across the trust in line with the Information Security Policy though may discharge elements of this function to the Trust Chief Technical Officer or another responsible individual. As part of this role they are responsible for:

- Undertaking relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to fulfil their role.
- Receiving reports relating to online safety incidents involving the central team.
- Meeting six times a year with the CTO to review standards and consistency across the schools and ensure all legislative requirements are met in respect of Broadband, Cyber and Filtering and Monitoring.
- Approving access requests for staff/ volunteers/ students and contractors working within the central team, in accordance with Appendix 3 of the trust Induction Policy (IT Network and Software Access).
- Receiving reports of Information Security Breaches and liaising with the DPO in instances of a personal data breach.
- Ensuring the receipt of Acceptable Use Agreements is logged on the school MIS or Single Central Register in the case of staff, volunteers, student teachers and contractors.
- Ensuring that all members of the central team:
    - Are made aware of the Online Safety Policy though the induction process and when the policy is updated have an awareness of current online safety matters/trends and any impact on current practices.
    - understand that online safety is a core part of safeguarding.
    - have read, understood, and signed the relevant acceptable use agreement (AUA).
    - understand that all digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems.
    - are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.

g. **Directors of Education are responsible for:**

- Overseeing the work of the Headteachers at each of their schools and holding them to account through provision of Headteacher reports three times a year which include online incidents and filtering information, and completion of the trust and LA Safeguarding audits, which will include completion of the 360-degree safe self-review tool.
- Ensuring that the Online Safety Policy is followed.
- Reporting to the School Improvement Committee on the level of online safety incidents and the annual review of the filtering and monitoring at their schools.

h. **Headteachers and Leadership Teams are responsible for:**

- Ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead or if appointed, the Online Safety Lead.
- Being aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Ensuring that the Designated Safeguarding Lead/Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

- Ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This would be the Director of Education for the school who would complete this through the LA and Trust Safeguarding audits and the Heads report which is completed three times a year.
- Receiving regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- Working with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring to ensure standards are met, decisions as to blocked content are documented and the effectiveness of provision is reviewed.
- Approving access requests for staff/ volunteers/ students and contractors working within their school, in accordance with Appendix 3 of the trust Induction Policy (IT Network and Software Access).
- Ensuring the receipt of Acceptable Use Agreements is logged on the school MIS or Single Central Register in the case of staff, volunteers, student teachers and contractors.

i. **Designated Safeguarding Leads are responsible for:**

- Holding the lead responsibility for online safety, within their safeguarding role.
- Receiving relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meeting regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual filtering and monitoring checks are carried out.
- Being responsible for receiving reports of online safety incidents and handling them, being aware of the potential for serious child protection concerns, deciding whether to make a referral by liaising with relevant agencies and ensuring that all incidents are recorded to inform future online safety developments.
- Liaising with Trust, Local Authority, IT Support Company, teaching staff, pastoral staff and support staff (as relevant) in respect of an incident.
- Liaising with staff and IT support providers on matters of safety and safeguarding and welfare (including online and digital safety).
- Ensuring that the IT support provider carries out all the online safety measures that the school's obligations and responsibilities require and follows and implements the trust Online Safety Policy and procedures.
- Reporting regularly to the Director of Education and senior leadership team.
- Reporting to Local Governance Committee meetings.

j. **The Online Safety Lead (as part of their role as DSL) is responsible for:**

- Working closely on a day-to-day basis with the Deputy Designated Safeguarding Lead (DSL).
- Receiving reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- Promoting an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- Liaising with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- Providing (or identifying the sources of) training and advice for staff/governors/ parents/ carers/pupils/student teachers/contractors and volunteers who have access to IT systems.
- Receiving regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined In Keeping Children Safe in Education – Content, Contact, Conduct and Commerce.

k. **Curriculum Leads are responsible for:**

- Working with the DSL/OSL to develop a planned and coordinated online safety education programme.
  This will be provided through a number of ways:
    - a discrete programme
    - PHSE and SRE programmes
    - A mapped cross-curricular programme
    - Assemblies and pastoral programmes
    - through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

l. **Teachers and Educational Support Staff are responsible for:**

- Ensuring that online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensuring that pupils understand and follow the Online Safety Policy and acceptable use agreements.
- Supervising and monitoring the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- Ensuring that in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are followed for dealing with any unsuitable material that is found in internet searches.
- Ensuring that where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- Ensuring that there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- Ensuring that they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media in line with the Trust Professional Behaviour, Expectations and Standards Policy.

m. **All Staff and Volunteers, including student teachers on placement and contractors with access to the school IT system are responsible for:**

- Ensuring that they have an awareness of current online safety matters/trends and of the current trust Online Safety Policy and practices through the Induction process.
- Ensuring that they understand that online safety is a core part of safeguarding.
- Ensuring they have read, understood, and signed the relevant acceptable use agreement (AUA).
- Ensuring that all digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems.

- Ensuring that they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures.
- Staff should make a report using the school Safeguarding online system for pupils, or for staff concerns, in accordance with the Allegation Flowchart Procedures when:
  - they witness or suspect unsuitable material has been accessed
  - they can access unsuitable material
  - there are teaching topics which could create unusual activity on the filtering logs
  - there is failure in the software or abuse of the system
  - there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
  - they notice abbreviations or misspellings that allow access to restricted material.

n. **The IT support provider is responsible for:**

- Ensuring that they are aware of and follow the trust Online Safety Policy to carry out their work effectively.
- Ensuring that the school technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensuring that the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from the trust or other relevant body.
- Ensuring that there is clear, safe, and managed control of user access to networks and devices following approval from Headteachers or CFOO.
- Ensuring that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Ensuring that the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL at the individual school for investigation and action.
- Ensuring that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see section 13 - Technical Security).
- Ensuring that any technical monitoring systems that are implemented are regularly updated as agreed.
- Ensuring that actions are completed following any concerns or checks to systems.
- Ensuring that regular consultant meetings are attended across the year with all Headteachers to review filtering and monitoring compliance, findings from Safeguarding audits and to support with completion of the 360-degree safe self-review tool if requested by school.
- CTO (Chief Technical Officer) to meet six times a year with CFOO to review standards and consistency across the schools and ensure all legislative requirements are met.
- Providing an annual report on the review of the filtering provision at each school to ensure the trust is compliant with DfE Filtering and Monitoring Standards.

o. **Pupils are responsible for:**

- Understanding that they must use the school digital technology systems in accordance with the pupil acceptable use agreement and Online Safety Policy (including personal devices – where allowed).
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understanding what to do if they or someone they know feels vulnerable when using online technology.

- Understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

p. **Parents and Carers**

Parents and Carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the Trust Online Safety Policy on the school website.
- providing them with a copy of the pupils' acceptable use agreement.
- publishing information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc (see parent/carer Acceptable Use Agreement in the appendix).
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to pupils in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed).

q. **Community users**

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user Acceptable Use Agreement before being provided with access to school systems. (A community user's acceptable use agreement template can be found in Appendix E).

The trust encourages the engagement of agencies/members of the community, for example PCSO's, who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

4. Professional Standards

a. There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

5. Acceptable Use

a. Acceptable Use Agreements outline the trust's expectations on the responsible use of technology by its users and will be highlighted as part of trust or school communications on a regular basis via:
   - School handbook.
   - Staff induction.
   - Posters and Notices displayed around the school.

- Communication with parents.
- Lessons.
- School Websites.
- Peer Support.
- Trust Newsletters.
- Trust Internal communications.

b. The relevant trust Acceptable Use Agreements, which can be found in the appendices at the end of this policy, should be signed by the relevant party and must be understood and followed.

c. The trust has defined what it regards as acceptable/ unacceptable use and this is shown in the tables below: -

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering **N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges**					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent pupils becoming involved in cyber-crime and harness their activity in positive ways– further information can be found here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: **Individual schools may wish to add further activities to this list.**	**Staff and other adults**					**Pupils**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Allowed during official breaks on own device	Not allowed	Allowed	Allowed at certain times, to be specified by class teacher	Allowed with staff permission
Online gaming					X	X			
Online shopping/commerce for personal use					X	X			
Online shopping for work purposes (orders must be placed in line with Financial Procedures Manual)		X				N/A			

External File Sharing to appropriate people		X				X			
Social Media for school/ trust purposes		X				X			
Social Media					X	X			
Messaging/ Chat for work purposes on Teams		X				X			
Messaging/ Chat for work purposes via Text, WhatsApp or similar			X			X			
Entertainment streaming e.g. Netflix, Disney +					X	X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok for work purposes		X				X			
	Staff and other adults					**Pupils**			
Consideration should be given for the following activities when undertaken for non-educational purposes: **Individual schools may wish to add further activities to this list.**	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Allowed during official breaks on own device	Not allowed	Allowed	Allowed at certain times, to be specified by class teacher	Allowed with staff permission
Mobile phones may be brought to school		X					X		
Smart Glasses may be brought to school	X					X			

Smart watches may be brought into school		X but pop up notifications must be removed and use of apps must only be used in designated staff areas.					X (Off and locked away)		
Use of mobile phones for learning at school		X				X			
Use of mobile phones in social time at school					X	X			
Taking photos on mobile phones/cameras		X				X			
Use of other personal devices, e.g. tablets, gaming devices					X	X			
Use of personal e-mail in school					X	X			
Use of personal email in school on school network/wi-fi	X					X			
Use of school email for personal e-mails	X					X			

d. When using communication technologies, the trust considers the following as good practice:
   - when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the trust.
   - any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses (except in respect of an email to the personal email address of a parent), text messaging or social media must not be used for these communications.*
   - staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
   - users should immediately report to the DSL/OSL or other nominated person – in accordance with the trust policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- relevant policies and permissions, including the Trust Professional Behaviours, Expectations and Standards policy should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff.

6. Reporting and Responding to Incidents

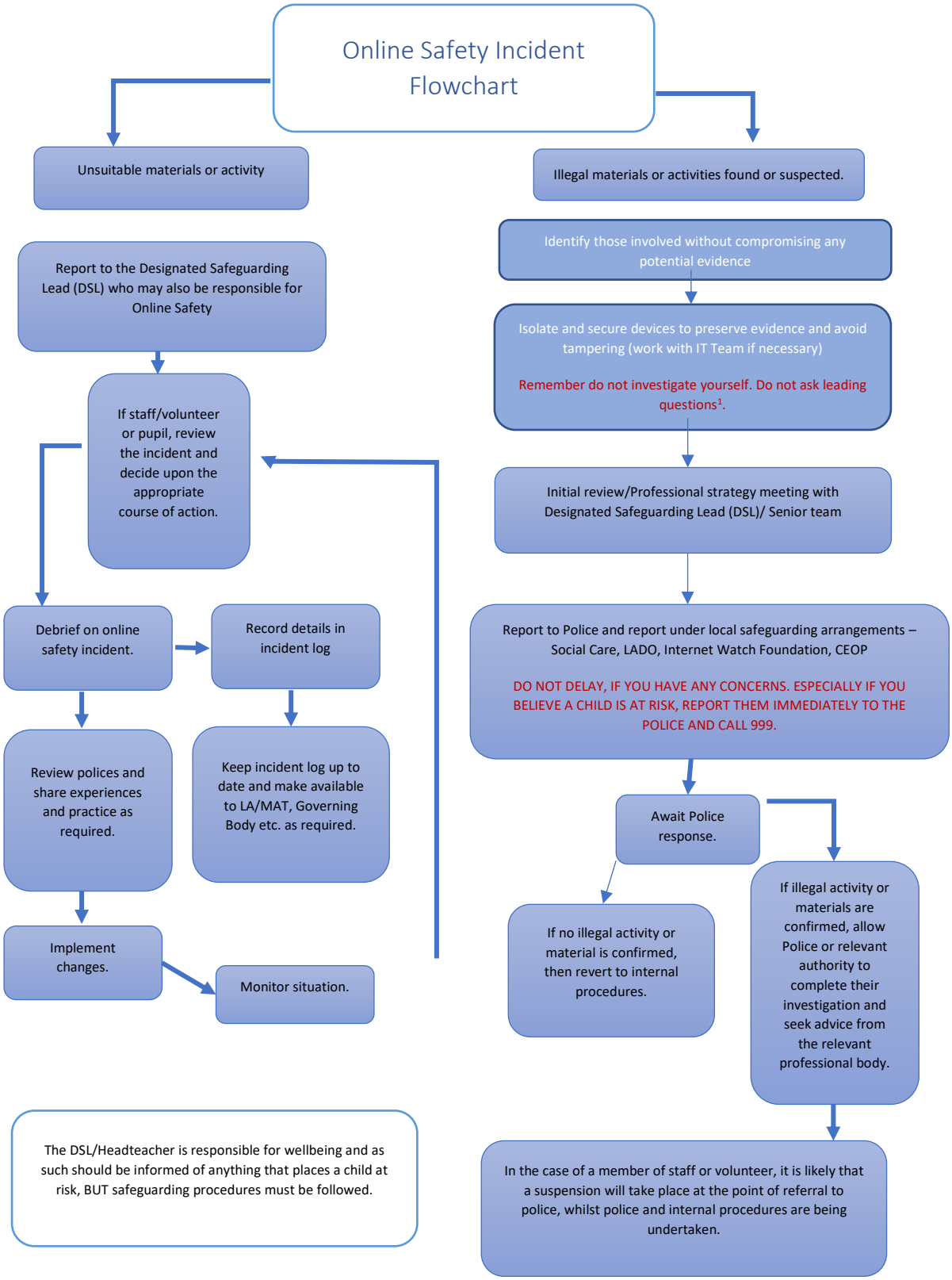
a. The trust will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of the school (with impact on the school and/ or trust) which will need intervention. The Trust and its schools will ensure that:
   - there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
   - all members of the school community will be made aware of the need to report online safety issues/incidents.
   - reports will be dealt with as soon as is practically possible once they are received.
   - the DSL, OSL and other responsible staff have appropriate skills and training to deal with online safety risks.
   - if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart below), the incident must be escalated through the agreed school safeguarding procedures, this may include:
     - Non-consensual images
     - Self-generated images
     - Terrorism/extremism
     - Hate crime/ Abuse
     - Fraud and extortion
     - Harassment/stalking
     - Child Sexual Abuse Material (CSAM)
     - Child Sexual Exploitation Grooming
     - Extreme Pornography
     - Sale of illegal materials/substances
     - Cyber or hacking offences under the Computer Misuse Act
     - Copyright theft or piracy.
   - any concern about staff misuse will be reported to the Headteacher/ CFOO or CEO, in accordance with line management responsibilities, unless the concern involves the Headteacher in which case the complaint is referred to the Chair of Governors and the CEO. Should the concern involve the CFOO, the complaint will be referred to the CEO and for the CEO, the complaint will be referred to the Chair of Trustees.
   - where there is no suspected illegal activity, devices may be checked using the following procedures:
     - more than one senior member of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
     - conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
     - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
     - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.

These may be printed, signed, and attached to the form (see Appendix H for a Record of Review form).

- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by the Trust
  - police involvement and/or action.

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- incidents should be logged either on the Reporting Log to be found in appendix I or on the Safeguarding System for the school.
- relevant staff are aware of external sources of support and guidance that are available, in dealing with online safety issues, especially to children and young people who are victims or who perpetrate harmful sexual behaviour, e.g. local authority and local safeguarding partnerships; police; Professionals Online Safety Helpline; Reporting Harmful Content.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - the Senior Leadership Team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
  - staff, through regular briefings
  - pupils, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
  - trustees and governors, through regular safeguarding updates
  - local authority/external agencies, as relevant.

b. The trust and all schools will use the flowchart below to support the decision-making process for dealing with online safety incidents.



c. **Trust Response to Actions**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as

possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupil Actions and Response

Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police/Social Work	Refer to IT Support Company for action re filtering, etc.	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X				
Attempting to access or accessing the school network, using another Pupil's account or allowing others to access school network by sharing username and passwords	X			X			X	
Attempting to access or accessing the school network, using the account of a staff member	X	X		X	X	X		
Corrupting or destroying the data of other users.	X	X		X	X	X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X			
Unauthorised downloading or uploading of files or use of file sharing.	X	X					X	
Using proxy sites or other means to subvert the school's filtering system.		X		X			X	
Accidentally accessing offensive or pornographic material and failing to report the incident.		X		X	X			

Deliberately accessing or trying to access offensive or pornographic material.		X		X	X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X			X			X	
Unauthorised use of digital devices – mobile phone/ digital camera or other mobile device (including taking images)	X	X			X			
Unauthorised use of social media/ messaging apps/ personal email	X	X		X	x			
Unauthorised use of non-educational sites in lessons	X						X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X			X			
Continued infringements of the above, following previous warnings or sanctions.	X	X			X			X

Staff Actions and Response

Incidents	Refer to line manager	Refer to Headteacher/ CEO	Refer to Police	Refer to IT Support Company for action re filtering, etc.	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X		
Deliberate actions to breach data protection or network security rules.		X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X
Using proxy sites or other means to subvert the school's filtering system.		X		X	X
Unauthorised downloading or uploading of files or file sharing	X	X		X	X
Breaching copyright or licensing regulations.	X			X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X			X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X			X
Using personal e-mail/social networking/messaging to carry out digital communications with pupils and parents/carers		X			X
Inappropriate personal use of school digital technologies e.g. social media / personal e-mail which would invalidate Cyber insurance	X			X	
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X			X	
Actions which could compromise the staff member's professional standing		X			X
Actions which could bring the school and trust into disrepute or breach the integrity or the ethos of the school and trust		X			X
Failing to report incidents whether caused by deliberate or accidental actions		X		X	
Continued infringements of the above, following previous warnings or sanctions.		X			X

7. Online Safety Education Programme

a. The trust recognises that while technical solutions are important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision as pupils need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

b. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

c. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. It will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against the National Curriculum regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Pupil need and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc.
- The curriculum incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- The programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. (Lessons and further resources are available on the CyberChoices site).
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. **Any request to do so, should be auditable, with clear reasons for the need.** This should be completed by following the flowchart in Appendix G.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes. The trust acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

8. Training

a. **Staff/ Volunteers/ University Placement Students and External Contractors**

- 'Keeping Children Safe in Education' states that:
  "All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

- All staff and relevant volunteers will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
    - a planned programme of formal online safety and data protection training will be made available to all staff and relevant volunteers. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
    - the training will be an integral part of the school's annual safeguarding and data protection training for all staff.
    - all new staff and relevant volunteers will receive online safety training and cyber security training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
    - the OSL and/ or DSL (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / LA / Trust / other relevant organisations) and by reviewing guidance documents released by relevant organisations
    - this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
    - the DSL/OSL will provide advice/guidance/training to individuals as required.

b. **Trustees/ Governors**

- Trustees and Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:
    - Online safety training as part of their induction and thereafter as stipulated by KCSIE and safeguarding requirements
    - Cyber-security training as part of their induction and annually thereafter
    - attendance at training provided by the local authority/Trust or other relevant organisation (e.g., SWGfL)
    - participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

- A higher level of training will be made available to (at least) the Online Safety Governor. This will include:
    - Cyber-security training (at least at a basic level)
    - Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

c. **Parents/ Carers**

- The trust recognises the essential role that parents and carers play in the education of their children and in the monitoring/ regulation of their online behaviours.
- The schools within the trust will seek to provide information and awareness to parents and carers through:
    - regular communication on online safety issues, curriculum activities and reporting routes
    - regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc

- pupils – who are encouraged to pass on to parents and carers, the online safety messages they have learned in lessons and by pupils leading sessions at parent/carer evenings. letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- sharing good practice with other schools in the trust.

d. **Community Groups**

- The trust encourages and supports schools to provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:
  - online safety messages targeted towards families and relatives.
  - providing family learning courses in use of digital technologies and online safety
  - providing online safety information via their website and social media for the wider community
  - supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision *(for example with an online safety review)*

9. Technology

a. All Trust Schools have an external technology provider who carries out the online safety and security measures on behalf of each school.
b. The provider must be fully aware of the Online Safety Policy and acceptable use agreements and each school must have a Data Processing Agreement in place with them alongside a Data Processing Impact Assessment.
c. Each school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that the procedures approved within this policy are implemented.
d. Each school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

10. Filtering and Monitoring

a. There is a filtering and monitoring system in place that safeguards staff and pupils by blocking harmful, illegal and inappropriate content.
b. The filtering and monitoring provision must be agreed at trust level and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. The Trust CFOO will work with the IT provider to agree review systems and procedures.
c. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

d. Checks on the filtering and monitoring system are carried out by the DSL at least annually as part of the filtering review with the involvement of a senior leader, the IT Service Provider and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access, or BYOD or new technology is

introduced. The Trust CFOO and CTO will work with the IT providers to agree the level of checks in place.

11. Filtering

a. Each school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
   The filtering system is up to date and applied to all:
   - users, including guest accounts
   - school owned devices
   - devices using the school broadband connection.

b. Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
c. There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
d. There is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix G for more details).
e. Filtering logs alert the Designated Safeguarding Lead and the DDSL to breaches of the filtering policy, which are then acted upon as soon as possible.
f. The trust and each school have provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils, etc.). Safesearch functionality must be enforced across all sites.
g. *younger pupils are encouraged to use child friendly/age-appropriate search engines e.g. SWGfL Swiggle as standard practice.*
h. access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
i. If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

12. Monitoring

a. The trust ensures monitoring systems are in place to protect each school, its systems and its users:
   - Each school monitors all network use across all its devices and services.
   - Monitoring reports are urgently picked up, acted on and outcomes are recorded by the DSL.
   - All users are aware that the network (and devices) are monitored.
   - There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising the response to alerts that require rapid safeguarding intervention.
   - Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
   - All trust schools follow the UK Safer Internet Centre Appropriate Monitoring guidance and protect users and school systems through the use of the appropriate blend of strategies informed by the highest level of risk assessed on the school's **360 safe template online** risk assessment. These may include:
     - physical monitoring (adult supervision in the classroom)
     - internet use is logged, regularly monitored and reviewed

- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, the IT support company at each school regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)
- taking account of pupil voice.

13. Technical Security

a. The trust is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities and that:

- Users can only access data to which they have right of access.
- Access to personal data is securely controlled in line with the Data Protection and Information Security policy.
- System logs are maintained and reviewed to monitor user activity
- There is effective guidance and training for users.
- There are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision.

b. The technical systems in each school will be managed in ways that ensure that the school meet recommended security requirements as determined by the trust:

- responsibility for technical security resides with the Trust IT Service Provider or School IT Service Provider where applicable who may delegate activities to identified roles.
- Cyber Security is included in the trust and school risk registers.
- there will be regular reviews and audits of the safety and security of school technical systems.
- servers, wireless systems and cabling are securely located and physical access restricted, there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud (Trust IT Support Provider).
- appropriate security measures in line with Cyber Security Standards (including updates) are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems. These are tested regularly.
- the school infrastructure and individual workstations are protected by up-to-date endpoint software to protect against malicious threats from viruses, worms, trojan etc.
- responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff of the Trust/ school IT support provider.
- all users have clearly defined access rights to school technical systems and devices and account are deleted when the user leaves. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the school SLT and CFOO for the central team.
- all school networks and systems will be protected by secure passwords. Password policy is consistent with guidance from the National Cyber Security Centre. (see section on password security in Appendix J).

- The IT Service Provider records the activity of users on the school technical systems and users are made aware of this in the acceptable user agreement. Any information would only be shared on request with Governors/ SLT/ DSL.
- the administrator passwords for school systems are kept in a secure place, e.g. those schools with Trust IT Support Provider have passwords secured with them in an offsite digital password vault. Other schools not with Trust IT Support Provider - school safe.
- there is a risk-based approach to the allocation of pupil usernames and passwords. (see 'Password Security Appendix J for more information).
- The Finance Manager at each school with support from the IT Support Provider are responsible for ensuring that all software purchased by and used by each school is adequately licenced and the IT Support Provider is responsible for ensuring that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the SLT/ Trust and School IT provider – see Appendix K Cyber Security Flowchart.
- use of school devices out of school is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- personal use of any device on the school broadband is regulated by acceptable use statements that a user consents to when using the network.
- staff members are not permitted to install software on a school-owned device without the consent of the SLT and IT service provider.
- removable media (for example USB sticks) are **not** permitted due to the security risks they pose.
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place to support the use of tablets such as iPad's and Surface Pro's.
- guest users, such as supply teachers and student placement teachers, are provided with appropriate access to school systems based on an identified risk profile.

14. Mobile Technologies (including BYOD/BYOT)

a. Mobile technology devices may be a school owned/provided or privately-owned smartphone, tablet, watch, notebook/laptop or other technology that usually has a similar functionality to mobile phones (for example the ability to send and/or receive notifications or messages via mobile phone networks or the ability to record audio and/or video) and the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

b. Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Pupils now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in pupils that will prepare them for the high-tech world in which they will live, learn and work.

c. The Trust recognised the growing availability of wearable technologies, including smart glasses, smart watches and other internet-enabled devices. These technologies may present safeguarding, privacy, data protection and online safety risks where they are capably of recording, storing, transmitting or accessing digital content.

d. Pupils, staff and visitors must not use wearable devices to record images, audio or video on school premises without appropriate authorisation.

e. Any concerns regarding the inappropriate use of wearable technology, including unauthorised recording, live streaming, image capture, cyberbullying or breaches of privacy, must be reported in accordance with the Trust's safeguarding and online safety procedures.

f. The school acceptable use agreements for staff, pupils and parents/carers include the use of mobile technologies.

g. The trust allows the following access for mobile devices:

	School devices			**Personal devices (excluding Smart Glasses)**		
	School owned and allocated to a single user	School owned for use by multiple users		Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes		Yes (Switched off and locked away during school hours)	Yes	Yes
Full network access	Yes	Yes		No	No	No
Internet only	No	No		No	Yes	Yes

h. The school has provided technical solutions for the safe use of mobile technologies in school:
- All school devices are managed though the use of Mobile Device Management software.
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access).
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
- For all mobile technologies on the school network, filtering will be applied to the internet connection and attempts to bypass this are not permitted.
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- All mobile devices on the school network are monitored.
- Education is provided to support responsible use.
- Personal use is not permitted.
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the

school may add software applications for use in a particular lesson. Periodic checks of devices will be made by the IT provider to ensure that users have not removed required apps.

- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to pupils on authorised devices once they leave the school. Any apps bought by the user on their own personal account will remain theirs.
- The changing of settings that would stop the device working as it was originally set up and intended to work is not permitted.

i. When personal devices are permitted:
   - Personal devices commissioned onto the school network are segregated effectively from school-owned systems.
   - use of personal devices for school business is defined in the acceptable use agreement.
   - Where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
   - AI-enabled image generation, facial recognition systems and wearable recording devices such as smart glasses, are not permitted.
   - Parents are permitted to seek permission for a child to bring a personal device into school which serves a medical purpose for a child. E.g. a diabetes monitor linked to a mobile phone and/or smart watch.
   - Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
   - The trust accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
   - The trust accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
   - The trust recommends that the devices have a protective case to help secure them as the devices are moved around the school.
   - Pass-codes or PINs must be set on personal devices to aid security.
   - Information, such as a trust email account, held on an personal device must be protected by multi-factor authentication.
   - The trust is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

j. Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition:
   - there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements.
   - Users are responsible for keeping their device up to date through software, security and app updates. Pickwick recommend that updates are completed within 14 days of their release in line with guidance from the DFE.
   - Users are responsible for charging their own devices and for protecting and looking after their devices while in the school.
   - Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.

- The expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- Printing from personal devices will not be possible.

15. Social Media

a. The trust recognises the widespread use and benefits of social media for professional and personal purposes.

b. Expectations for teacher's professional conduct are set out in the DfE Teacher Standards but all adults working should understand the nature and responsibilities of their workplace puts them in a position of trust and their conduct in respect of social media should reflect this.

c. The trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils though:
    - ensuring that personal information is not published.
    - education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
    - clear reporting guidance, including responsibilities, procedures, and sanctions.
    - risk assessment, including legal risk.
    - guidance for pupils, parents/carers.

d. Please see the trust Professional Behaviours, Expectations and Standards for more details.

16. Digital and Video Images

a. The trust recognise that the development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

b. However, such images provide avenues for online bullying to take place and therefore the trust must provide guidance on the use and the risk of Digital and Video images across its schools.

c. The trust will ensure that each of its schools will inform and educate users about the risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. (Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education).
- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those pupils whose images must not be taken/published. Those images should only be taken on school devices.
- personal devices of staff should not be used for such purposes

- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not 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.
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- care should be taken when sharing digital/video images that pupils are appropriately dressed.
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with Online Safety Policy requirements in section 18 below.
- written permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media. (see parents and carers acceptable use agreement in Appendix C). Permission is not required for images taken solely for internal purposes.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the Trust Records Management Policy.
- images will be securely stored in line with the Trust Records Management Policy.
- pupils work can only be published with the permission of the pupil and the parents/ carers.

17. Online Publishing

a. The trust and each school communicate with parents/carers and the wider community and promote each school through:
   - Public-facing website.
   - Social media.
   - Online newsletters.

b. The website of the trust and each school is managed/hosted by an approved provider. The school ensures that the online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is the least risk to members of the school community, through such publications.

c. Where pupil work, images or videos are published, their identities are protected, and full names are not published.

d. The trust public online publishing (trust or school website) provides information about online safety e.g., publishing the trust Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on each school website.

18. Children's' Images and Emerging Technologies

a. The Trust recognises that photographs and video images of pupils constitute personal data and may present safeguarding risks when published online. In addition to traditional online risks, advances in artificial intelligence (AI), facial recognition technology and image manipulation tools increase the potential for children's images to be copied, altered, misused or redistributed without consent.

b. Before publishing pupil images on Trust websites, social media platforms or promotional materials, the Trust will consider both data protection requirements and safeguarding implications. Wherever practicable, the Trust will:

- minimise the use of identifiable facial images by replacing close-up individual images with more activity-based or angled photographs, and using lower resolution images;
- avoid publishing pupils' full names alongside photographs;
- use group images in preference to individual portraits;
- apply privacy settings to help limit who can view and share content;
- remove metadata from images that may reveal a location, device or timestamp;
- ensure image use accords with published privacy information and parental preferences;
- remove or archive images when they are no longer required by reviewing website content biannually;

c. The Trust reserves the right not to publish, or to remove, any image of a pupil where there are safeguarding concerns or where publication may increase the risk of identification, exploitation, unauthorised image manipulation, or other harm.

19. Data Protection

a. Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

b. The trust:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO).
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place for each school and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The trust Records Management Policy and 'retention schedule" supports this.
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.

- provides staff, parents and volunteers, with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them.
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier.
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a Data Breach policy for reporting, logging, managing, investigating and learning from information risk incidents.
- has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- provides data protection training for all staff at induction and appropriate refresher training thereafter.

c. When personal data is stored on any mobile device the:
- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software.
- data will be securely deleted from the device, in line with trust policy (below) once it has been transferred or its use is complete.

d. Staff must ensure that they:
- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school.
- only use encrypted data storage for personal data.
- will not transfer any school personal data to personal devices. Procedures are in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

20. Equal Opportunities

a. An Equality and Diversity Impact Assessment has been completed in order to ensure this policy complies with equality obligations outlined in discrimination legislation. We believe the policy positively reflects the aims and ambitions identified in the trust Single Equality Scheme. The policy positively reflects the aims and ambitions of Pickwick Academy Trust.

22. Legislation

a. This policy is based on the latest version of Keeping Children Safe in Education, the SWGFL Online Safety Policy template and has due regard to legislation and statutory guidance including, but not limited to:

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Criminal Justice and Public Order Act 1994
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964
- Human Rights Act 1998
- The Education Act 2006
- The Education Act 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- Serious Crime Act 2015
- Criminal Justice and Courts Act 2015

20. References, acknowledgements and associated documents

- This policy will be implemented in conjunction with all other Pickwick Academy Trust policies (please see Scheme of Delegation for full list) including:
    - Data Protection
    - Information Security
    - Data Breach
    - Records Management
- and is in the same group as the following policies:
    - Safeguarding and Child Protection
    - Behaviour
    - Whistleblowing
    - Relationships. Sex and Health Education/ PSHE
    - Professional Behaviours, Expectations and Standards

21. All policies are available to view by contacting the school or Trust offices

22. Appendices

A Pupil Acceptable Use Agreement Template – KS2
B Pupil Acceptable Use Agreement Template – for younger pupils (Foundation/KS1)
C Parent/Carer Acceptable Use Agreement Template
D Staff (and Volunteer) Acceptable Use Policy Agreement Template
E Community Users Acceptable Use Agreement Template
F Filtering and Firewall change process
G Record of reviewing devices/internet sites (responding to incidents of misuse)
H Online Safety Incident Reporting log
I Password Security
J Cyber Security Concern/ Personal Data Breach – Action to Take

Appendix A –

Pupil Acceptable Use Agreement Template – for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Pupils should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that pupils will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help pupils to understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of “stranger danger” when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do as advised to me by my teacher.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones etc.) in the school if I have permission. If I am allowed, I still have to follow all the other school rules if I use them.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

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

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules there maybe a consequence linked to the school Behaviour policy.

Pupil Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

(Schools have the option to decide if they require pupils or parents/carers to sign the form at the start of KS2, or whether they wish to simply make them aware of its contents through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Pupil: ..... Class: .....

Signed: ..... Date: .....

Parent/Carer Countersignature (optional)

Name of Parent/Carer: .....

Signed: ..... Date: .....

Appendix B –

Pupil Acceptable Use Agreement Template – for younger Pupils (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Signed (parent/ carer): .....

(Schools have the option to decide if they require pupils to sign the form at the start of KS2, or whether they wish to simply make them aware of its contents through education programmes/awareness raising).

Appendix C –

Parent/Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people 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 parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name: .....

Pupil Name/s: .....

As the parent/carer of the above pupils, I give permission for my child/ children to have access to the digital technologies at school.

(KS2 and above)

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

And/ Or: (KS1)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and

systems**. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.**

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child/ children to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	
Who will have access to this form.	
Where this form will be stored.	
How long this form will be stored for.	
How this form will be destroyed.	

Signed: .....

Date: .....

Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the pupil acceptable use agreement.

Appendix D –

Staff (including Volunteer, University Placement Students Placement and External Contractors) Acceptable Use Policy Agreement Template

Trust 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, AII will 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 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 school 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 trust/ school will monitor my use of the school 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 trust/ school, and to the transfer of personal data (digital or paper based) out of trust/ school
- I understand that the trust/ school digital technology systems are primarily intended for educational use and that I will not use the systems for personal or recreational use
- 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 trust 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 trust/ 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 (e.g. 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 trust'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 share my personal email address/ phone number or details of my personal social networking details.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The trust has the responsibility to provide safe and secure access to technologies and ensure the smooth running of each school:

- When I use my mobile devices in school or to access my school/ trust email account outside of trust settings, I will follow the rules set out in this agreement and policy, in the same way as if I was using school equipment. I will also follow any additional rules set by the trust 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 only use my mobile phone in line with the requirements of the policy and will ensure that any pop-up notifications are removed from my smart watch.
- I will not use personal email addresses on the school's 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). Should I inadvertently click on an attachment that looks suspicious I will follow the instructions contained in Appendix K – Cyber Security Concern or Personal Data Breach.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist 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 trust/ school policies.
- I will not disable or cause any damage to school 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 trust Data Protection Policy Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the trust 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.
- **If I have been provided with school/ trust equipment for my use for work purposes:**
    - **I will only use it for work purposes;**
    - **If the equipment is lost, damaged or stolen I will report it immediately to my line manager/Headteacher;**
    - **When I leave the company, I will return the equipment in good working order;**
    - **I lose or fail to return the equipment, or it is damaged beyond normal wear and tear due to negligence on my part, I authorise payroll to deduct the cost of a reasonable replacement from my salary.**

- When using the online systems in my professional capacity:

  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 the trust/ school's digital technology equipment in school settings, but also applies to my use of trust/ 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 trust/ school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension or referral to the CEO or Trustees as part of a Disciplinary process and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer/ Student/Contractor Name: .....

School/ Central Team: .....

Equipment Details (if applicable)

Make …….

Model …….

Serial Number …….

Asset Number …….

Additional Description

……

Signed: .....

Date: .....

Appendix E -

Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- 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 if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

As the school is collecting personal data by issuing this form, it should inform community users about:

Who will have access to this form.	How this form will be destroyed.
Where this form will be stored.	How long this form will be stored for.

Name: .....

Signed: .....

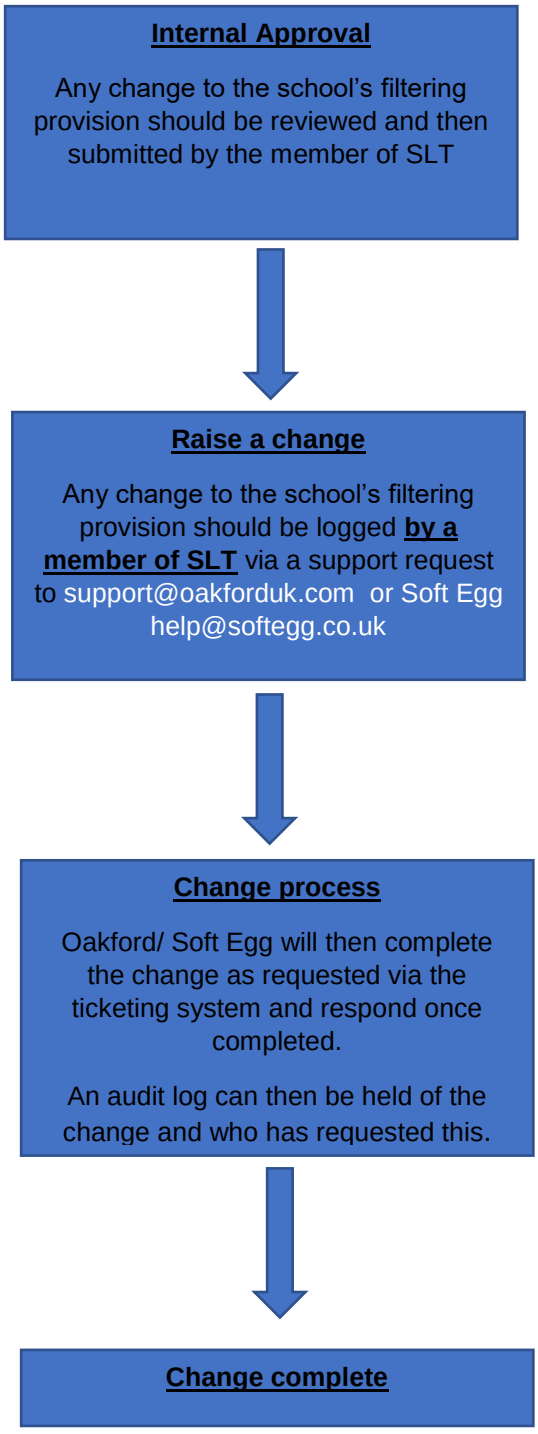
Date: .....

Appendix F

Filtering and Firewall change process

The following document outlines the filtering and firewall change process to be followed by the school in the event of a change required.

Filtering Change



Firewall Change



Regular Change Review

The school should maintain documented process to ensure that Filtering and firewall rules are reviewed every 12 months minimum.

Appendix G

Record of reviewing devices/internet sites (responding to incidents of misuse)

School/ Central Team	
Date of Review	
Reason for Investigation	
Details of First Reviewing Person	
Name	
Position	
Signature	
Details of Second Reviewing Person	
Name	
Position	
Signature	
Name and Location of Computer Used for Review of Websites	
Website address (URL)	**Reason for Concern**
Conclusion	

Action proposed or taken	**Action holder**	**Target date of completion**

Appendix H

Online Safety Incident Reporting Log

School/ Central Team : .....

Incident	*Action Taken*		*Incident Reported By*	*Signature*
	What?	*By Whom?*		

Appendix I

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform) - National Cyber Security Centre The password policy and procedures reflect NCSC and DfE advice/guidance.

- The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.
- Security measures are in place to reduce brute-force attacks and common passwords are blocked.
- School networks and system will be protected by secure passwords.
- Passwords are encrypted by the system to prevent theft.
- Network Access passwords do not expire and the use of password managers is encouraged.
- Complexity requirements (e.g. capital letter, lower case, number, special character) are not used.
- Users are able to reset their password themselves.
- All passwords are at least 12 characters long and users are encouraged to use 3 random words.
- Passwords are immediately changed in the event of a suspected or confirmed compromise.
- No default passwords are in use. All passwords provided “out of the box” are changed to a unique password by the IT Service Provider.
- All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods.
- A copy of administrator passwords is kept in a secure location.
- All users (adults and pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.

Pupil passwords:

Schools take a risk-based approach to the allocation of pupil usernames and passwords.

- For younger children and those with special educational needs, usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. These are set as a minimum of X characters.
- Pupils are encouraged to set passwords with an increasing level of complexity. Passwords using 3 three random words and with a length of over 12 characters are considered good practice.
- Users will be required to change their password if it is compromised. (Note: passwords should not be regularly changed but should be secure and unique to each account.)
- Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important. The Project EVOLVE Privacy and Security strand supports with this.
- Alternative authentication methods are used where possible.
- Access for pupils to the network is separate from secure areas.

Appendix J

CYBER SECURITY CONCERN and / or PERSONAL DATA BREACH – Action to take

(Updated September 2023)

I have received an email that looks suspicious and think it might be a phishing email.	I have received an email that looks suspicious, and I have clicked on the attachment.	I have received an email that looks suspicious, I have clicked on the attachment and entered personal information, login details or password.	I have sent personal data without a password to the wrong person.
DO NOT click on the attachment, forward it to Oakford Technology with an explanatory note – support@oakforduk.com Or to Soft Egg help@softegg.co.uk	Call Oakford Technology immediately on **01380 888088** **Or** **Soft Egg - 0800 999 1212** Inform your line manager.	Call Oakford Technology immediately on **01380 888088** **Or** **Soft Egg - 0800 999 1212** Inform your line manager	Advise Line Manager Complete Data Incident Reporting Form and send to Head. Head to send to CFOO and DPO - i-west@bathnes.gov.uk
	Whilst waiting for the helpdesk to speak to you, if you spot unusual activity on your device, disconnect the broadband by clicking on the symbol below, found in the bottom right hand corner of your screen and selecting disconnect	Whilst waiting for the helpdesk to speak to you, if you spot unusual activity on your device, disconnect the broadband by clicking on the symbol below, found in the bottom right hand corner of your screen and selecting disconnect	
DO NOT forward the email to other staff	DO NOT forward the email to other staff	DO NOT forward the email to other staff	
The IT Support desk will usually request that you mark the item as "Junk" and they will make an adjustment to block future receipt	Your IT Support desk will request access to your machine to investigate the issue and view the email and attachment. They will decide on the appropriate action. Your IT Support Company may implement a forced password change and will contact the DPO and inform them of the initial investigation.	Your IT Support desk will request access to your machine to investigate the issue and view the email and attachment. They will decide on the appropriate action. Your IT Support Company may implement a forced password change and will also contact the DPO and inform them of the initial investigation.	
	A report will be completed by your IT support provider and a copy provided to the DPO and CFOO within 48 working hours of the reported event.	Personal Data Breach Protocol followed Data Incident Reporting Form to be completed	

If you are concerned that something has happened out of hours please stop work, do not switch off your device and contact your IT Provider as soon as they re-open for advice/assistance – follow guidance below

Actions in the event of a suspected Cyber-Attack

1. In the event of a suspected cyber-attack, staff should isolate devices from the network by either unplugging the network cable from the back of the laptop or PC, or by clicking on the icon at the bottom of the screen on the right-hand side that looks like  and clicking on airplane mode.
2. In order to assist data recovery, if damage to a computer or back up material is suspected, staff **should not:**
    - Turn off electrical power to any computer.
    - Try to run any hard drive, back up disc or tape to try to retrieve data.
    - Tamper with or move damaged computers, discs or tapes.
3. Contact IT support company(Soft Egg 0800 999 1212)
4. Contact your line manager and the Business Director (01249 717090)
5. Contact RPA Emergency Assistance Helpline - **0800 368 6378**
6. Convene the Cyber Recovery Team (CRT) who will:
7.

- Start the Actions Log to record recovery steps and monitor progress. (From Cyber Response Plan)
- Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
- Assess and document the scope of the incident using the Incident Impact Assessment at Appendix A to identify which key functions are operational / which are affected.