Online Safety Policy

Review by policy owners:	Ben Croton, Suzie Jones (Online safety policy review group), December 2022 Kate Woodhead (Director of Operations), James Bushby (IT Lead), January 2023
Review by Trustees:	James Hannam and Gaynor Brown, January 2023
Ratified by Board of Trustees:	25 January 2023 (Education Committee)
Next review date:	For Spring Full Board of Trustees 2024

Within this policy the term CEO refers to the CEO of the Trust. The term Headteacher refers to the Headteacher of the School (or Executive Headteacher where applicable). For any matters relating to staff who work outside of a single school setting, the Head of Service is the responsible person where the term “Headteacher” is used. If an issue / potential issue is connected with a Headteacher or Head of Service, the CEO is the responsible person where the term “Headteacher” is used.

The Trustees of the Twynham Learning Trust (the Trust) are Charity Trustees and Company Directors and for the purpose of this policy these terms are interchangeable.

This policy reflects the legislation at the time that it was last reviewed. Any changes in legislation will take precedence over anything printed in this policy.

Contents

1. Statement of intent

Twynham Learning understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout schools; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Twynham Learning has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

2. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) ‘Harmful online challenges and online hoaxes’
- DfE (2022) ‘Keeping children safe in education 2022’
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
- DfE (2019) ‘Teaching online safety in school’
- DfE (2018) ‘Searching, screening and confiscation’
- National Cyber Security Centre (2018) ‘Small Business Guide: Cyber Security’
- UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’

This policy operates in conjunction with the following Trust-wide (T) and School (S) policies:

- Child Protection and Safeguarding Policy (T)
- Child Protection Procedures (S)
- Data Protection Policy (T)
- Special Educational Needs and Disabilities (SEND) Policy (T)
- Behaviour Policy (S)
- Anti-Bullying Policy (S)

- Code of Conduct for Staff & Volunteers (T)
- Relationships and Sex Education Policy (T)
- Staff Discipline Policy & Procedure (T) – only available to Staff
- Remote Learning Policy (T)

3. Scope of the Policy

This policy applies to all parts of Twynham Learning, including staff, pupils, volunteers, parents / carers, governance volunteers, visitors and community users who have access to and are users of the trust's infrastructure, both on and away from our school sites.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

4. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

4.1 Local Advisory Board (LAB) members and Trustees

LAB members and Trustees are responsible for monitoring the Online Safety Policy and for reviewing its effectiveness. Regular information about online safety incidents and monitoring reports will be provided to them. The LAB will appoint one of its members to hold a linking role on Safeguarding which includes Online Safety; some LABs may decide to appoint a second member with a separate Online Safety role. In either scenario, the LAB member will:

- Be in regular contact with the Online Safety Coordinator
- Attend appropriate Safeguarding / Online Safety meetings
- Regularly monitor online safety incident logs
- Report to the LAB as appropriate

4.2 Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the DSL and/or Online Safety Coordinator.

- The Headteacher and Senior Leadership Team (SLT) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of

staff set out in Section 8 “Responding to incidents of misuse” and with relevant HR policy / procedures
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles, and to train other colleagues as required
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those who carry out the internal online safety monitoring role. This is to provide a safety net and also give appropriate support to those colleagues whose wellbeing may be impacted by what they deal with.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator / DSL.

4.3 Designated Safeguarding Lead

The DSL will be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

4.4 Online Safety Coordinator

The activity of an Online Safety Coordinator is key in every school but the Headteacher has discretion to include the activity within the existing DSL / DDSL team or to create a separate role, depending on local circumstances. The Online Safety Coordinator will:

- Ensure that the school’s Safeguarding meetings cover the preventative and reactive aspects of Online Safety
- Take responsibility for online safety issues and have a leading role in establishing and reviewing the school’s online safety documentation and arrangements (including the formation of an Online Safety Group if this is required in addition to the safeguarding oversight and governance arrangements)
- Map and review the online safety curricular provision – ensuring relevance, breadth and progression
- Liaise with the DSL (if a separate role has been created)
- Ensure that all staff are aware of the procedures to be followed in the event of an online safety incident
- Provide training and advice for staff
- Liaise with Trust Core Services / school IT Technicians in order to address risks and issues
- Ensure that the Trust’s incident log is maintained to inform future online safety developments
- Liaise regularly with the relevant link LAB member to discuss current issues, review incident logs and new control measures
- Report regularly to Senior Leadership Team
- Work closely with the police during their investigations (under SLT direction)
- Consult stakeholders (including parents / carers and pupils) about the online safety provision
- Monitor improvement actions identified through use of the self-assessment / review tools and audits

4.5 Technical IT Staff

Twynham Learning's technical infrastructure is designed and maintained centrally by Core Services but with school-focussed Technicians supporting each school's users in terms of account creation and hardware support. The technical IT support staff are expected to work together as a matrix team across the Trust in matters of Online Safety, irrespective of organisational boundaries.

The Trust's IT Lead is responsible for ensuring:

- That the Trust's technical infrastructure is secure and is not open to misuse or malicious attack
- That the Trust's technical infrastructure meets required online safety technical requirements and any other relevant body Online Safety Policy or Guidance that may apply
- That monitoring software and systems are utilised to ensure the effective functioning of the network in its protection of users
- That they provide support to online safety incidents if independence from the school's arrangements or personnel is required

IT Technicians are responsible for ensuring:

- That users may only access the networks and devices through a properly enforced and sufficiently strong password protection policy
- 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, working through Core Services to communicate risks and issues consistently across the Trust
- That the use of the network/internet/Gateway/remote access/email is regularly monitored (as a minimum through a weekly safeguarding report) in order that any misuse or attempted misuse can be reported for investigation and action or sanction as appropriate.

4.6 Teaching and Support Staff (including volunteers)

Teaching and support staff (including volunteers) are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the Trust's current arrangements
- They have read, understood and signed the relevant Acceptable Use Agreement
- They report any suspected misuse or problem to the DSL / DDSL for investigation and action or sanction
- All digital communications with pupils or parents / carers should be on a professional level and only carried out using approved school systems (usually through the Management Information System or email)
- Online safety issues are embedded in all relevant aspects of the curriculum and other activities
- Pupils understand and follow this Online Safety Policy and their Acceptable Use Agreement
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They act as good role models in their use of digital technologies, the internet and mobile devices
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and enforce current policies with regard to these devices
- During lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes must be in place for dealing with any unsuitable material found in internet searches

- Where pupils need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked, staff can request via a Helpdesk ticket that the local Technician can temporarily remove those sites from the filtered list for the period of study (the request must include clear reasons for the need).
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

4.7 Pupils

Whilst the practicalities of the following section will vary according to the pupil's age and understanding, the following standards are expected of pupils, who:

- Are responsible for using the school digital technology systems in accordance with their Acceptable Use Agreement
- Are responsible for seeking help from school staff if they are concerned about something they or a peer have experienced online
- Are responsible for reporting online safety incidents and concerns
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and on cyber-bullying
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Online Safety Policy covers their actions out of school, if related to their membership of the school

4.8 Parents and Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Parents will be encouraged to support the Trust in promoting good online safety practice and to follow guidelines as set out in the Acceptable Use Agreement on matters including, but not limited to:

- Digital and video images taken at school events
- Access to parents' sections of the website/Gateway and online pupil records

5. Education and training

5.1 Education – Pupils

Whilst regulation and technical solutions are very important, educating pupils to take a responsible approach to online safety is essential. Children and young people need the help and support of their school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities, and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / Computer Science / Personal Development (PSHE) / other lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils are helped to understand the need for their Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

5.2 Education – Parents and Carers

Parents / carers play an essential role in the education of their children and in the monitoring and regulation of children’s online behaviours. However, keeping up-to-date with the ever-changing online safety risks and issues is a real challenge. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Schools (individually or as clusters / phases) will therefore seek to provide information and awareness to parents through:

- Curriculum activities
- Parent information evenings
- Newsletters
- A dedicated Online Safety website portal via the school website

5.3 Education – The Wider Community

The Trust will provide opportunities for local community groups / members of the community to gain from the Trust’s online safety knowledge and experience. In addition to content freely available on school websites, this may be offered from time to time through:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents

5.4 Education & Training – Teaching and Support Staff (including volunteers)

It is essential that all staff 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 training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand this Online Safety Policy and Acceptable Use Agreement
- It is expected that some staff will identify online safety as a training need within the performance management process
- The Online Safety Coordinator / DSL (or other nominated person) will receive regular updates through attendance at external training events 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 Online Safety Coordinator / DSL (or other nominated person) will provide advice / guidance / training to individuals as required

5.5 Training – Trustees and LAB members

LAB members should take part in online safety training / awareness sessions, which may be offered in a number of ways:

- Undertaking training provided by the National Governors Association or other relevant organisation
- Participation in Trust or school training / information sessions for staff or parents (this may include attendance at assemblies / lessons)

6. Technical infrastructure

Twynham Learning will be responsible for ensuring that the Trust’s infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- Technical infrastructure will be managed in ways that ensure they meet recommended technical guidelines for safe operation
- There will be regular checks, reviews and audits of the safety and security of infrastructure
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users (staff, pupils and governance volunteers) will have clearly defined access rights to systems and devices
- All users (staff, pupils and governance volunteers) will be provided with a username and secure password by their local IT Technician as part of their onboarding / transition arrangements. Users are responsible for the security of their username and password
- System Admin passwords are tightly controlled and restricted to three members of technical staff only
- Technicians have both an individual Admin Accounts (for auditable changes to the system) and an individual User Account (for their general work)

- For central licensing (eg Microsoft), the Trust's IT Lead is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. For local licensing, the relevant IT Technician takes this responsibility
- Internet access is filtered for all users whilst on school premises. Illegal content (e.g. child sexual abuse images) is filtered by the web filter; content lists are regularly updated and internet use is logged and regularly monitored. Requests to deal with filtering changes must be made through the Trust's Helpdesk to ensure an audit trail remains
- The Trust's internet filtering helps to ensure that children are safe from terrorist and extremist material when accessing the internet and the spam filter protects email users from inappropriate content, cyber attacks and viruses.
- The Trust has provided enhanced / differentiated user-level filtering, allowing different filtering levels for different ages/stages and different groups of users – staff/pupils etc.
- Twynham Learning technical staff regularly monitor and record the activity of users on the Trust infrastructure and users are made aware of this in the Acceptable Use Agreements
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of systems and data. These are tested regularly. Infrastructure and devices are protected by up to date anti-virus software and system updates
- An agreed procedure is in place for the provision of temporary access of 'guests' (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- An agreed procedure is in place regarding the extent of personal use that users (staff/pupils/volunteers) and their family members are allowed on Trust devices that may be used away from school sites
- An agreed procedure is in place that controls the extent to which staff can download executable files and install programs on school devices (for general users, the system configuration prohibits this)
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks) by users on Trust devices. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

7. Use of Personal / Mobile Technologies & Social Media

7.1 Mobile Technologies

Modern technology enables many individuals to have device(s) about their person. It is likely that staff, volunteers, pupils and visitors will have mobile phones, tablets, laptops, wearable technology etc with them as they arrive at school. Some devices will be owned by the organisation and some will be owned by the individual / family. Generally, Twynham Learning's devices will be allocated to staff or be available within IT Suites / Laptop Trollies. However, there are occasions when devices will be allocated to pupils (from Twynham Learning purchase, from DfE supply, provided for meeting SEND / individual circumstances via a grant or donation) and, in those circumstances, the devices will be configured to access the appropriate parts of the network infrastructure, rather than be treated as a guest device.

Twynham Learning's wireless network is primarily in place for teaching and learning but there is provision for guests (including pupils, volunteers, visitors), utilising their own devices. If staff have personal devices in school, they can also utilise the guest wireless network. Much of Twynham Learning's technology provision (which is increasingly cloud-based) is also accessible via apps or a through a browser so that users can access it wherever they need and on whichever device they choose.

Staff are, however, encouraged to use work devices for work and, as a minimum, to ensure data is not downloaded to personal devices.

Whilst devices are prevalent in schools, it is important to state that the primary purpose of the use of mobile/ personal devices in a school context is educational. Their use must be in line with other relevant Trust or school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-bullying Policy, Acceptable Use Policy and Device Loan Agreement. Teaching about the safe and appropriate use of mobile technologies must be an integral part of each school's Online Safety education programme.

Appropriate sanctions can be imposed in line with the Behaviour Policy (for pupils) or Staff Discipline Policy & Procedure (for staff) for any contravention of school arrangements.

The Trust's Acceptable Use Agreements for staff, pupils, parents / carers and volunteers will give consideration to the use of mobile technologies.

7.2 Use of Digital Images

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. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term (it is common for employers to carry out internet searches for information about potential and existing employees). The Trust will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Parents / carers will be given the opportunity to opt out of consenting for photographs of their child to be published. Staff / volunteers will be given the opportunity to opt out of consenting for photographs of themselves to be published.
- In accordance with guidance from the Information Commissioner's Office, parents 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 made publicly available on social networking sites, nor should parents 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 Trust and school policies concerning the sharing, distribution and publication of those images. Images of people should only be taken on Twynham Learning equipment; the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital /video images to ensure that pupils are appropriately dressed and that the subjects of the image are not participating in activities that might bring themselves or the Trust into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Pupils' work can only be published with the permission of the pupil and parents
- Recordings of video calls, in person or online meetings etc without consent is not permitted

7.3 Data Protection

This is covered separately in the Data Protection Policy, which includes guidance relating to online safety.

7.4 Communication Technologies

Many staff and other adults will have mobile phones in school. Some staff will require to use a mobile as part of their work (including being "on call") but staff are not otherwise generally permitted to use their mobile phones during lessons. They are able to utilise them during schools within the confines of this policy for work purposes and during their break times.

It is recognised that those pupils who travel independently to school will often have a mobile phone with them and this is accepted. However, during school hours, pupil phones must be switched off and out of sight. Some Primary phase schools may have an additional requirement that phones are handed to the office or to a class teacher to be locked away and returned at the end of the day.

Sixth Form pupils may be given more flexibility to use mobile phones outside of lesson times and are therefore permitted to connect to the wireless provision.

Communication Technologies	**Staff & other adults**				**Pupils** (Primary & Secondary)				**Pupils** (Sixth Form only)			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	✓				✓				✓			
Use of mobile phones in lessons				✓				✓				✓
Use of mobile phones in break / social time (pupils), during breaks from work (all staff)	✓							✓		✓		
Use of mobile phones for work			✓									
Taking photos on mobile phones / cameras		✓						✓		✓		
Use of other mobile devices e.g. tablets	✓							✓			✓	
Use of personal email addresses in school, or on school network	✓							✓		✓		
Use of school email for personal emails				✓				✓				✓
Use of messaging apps	✓							✓		✓		
Use of social media	✓							✓		✓		
Use of blogs	✓							✓		✓		

When using communication technologies, the Trust considers the following as good practice:

- The Trust's email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person 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
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, online learning platforms etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Pupils will be provided with individual school email addresses for educational use
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

7.5 Social Media - Protecting Professional Identity

The Trust and its schools have a duty of care to provide a safe learning environment for pupils and staff. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the Trust liable to the injured party. The Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the Trust through:

- Ensuring that personal information is not published
- Providing training including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Staff should ensure that:

- No reference is made in their personal social media to pupils, parents or colleagues / volunteers
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or the Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- Approval by the Headteacher for its creation
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

The school's use of social media for professional purposes will be checked regularly by the Headteacher and/or DSL to ensure appropriateness and compliance

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the Trust or the school or impacts on the Trust or the school, it must be made clear that the member of staff is not communicating on behalf of the Trust or the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the Trust or the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The Trust permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the Trust or the school
- The Trust or the school should effectively respond to social media comments made by others according to a defined policy or process

8. Responding to incidents of misuse

8.1 Unsuitable / Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from Trust and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which, whilst they may be legal, are considered inappropriate in a school context, either because of the age of the users or the nature of those activities.

The Trust believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the school when using school equipment or systems. The Trust policy restricts usage as follows:

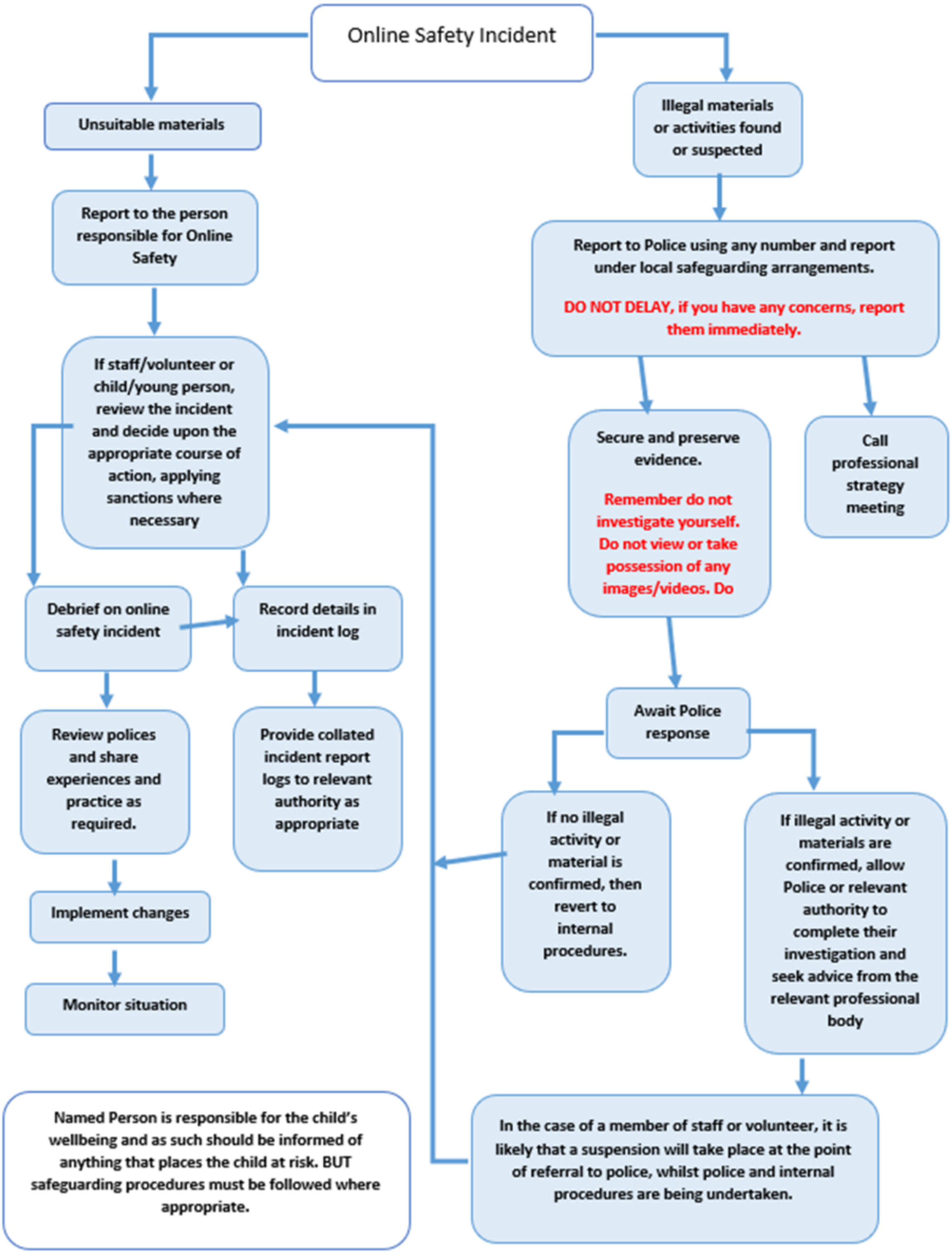
User Actions		Unacceptable and illegal	Unacceptable	Acceptable at certain times	Acceptable for nominated users	Acceptable at all times for all users
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978	✓				
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.	✓				
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008	✓				
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986	✓				
	Pornography		✓			
	Promotion of any kind of discrimination	✓				
	Threatening behaviour, including promotion of physical violence or mental harm	✓				
	Promotion of extremism or terrorism	✓				
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Trust or brings the Trust into disrepute		✓			
Using Trust systems to run a private business or selling any items / services for personal gain			✓			
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust			✓			
Infringing copyright		✓				
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)			✓			
Creating or propagating computer viruses or other harmful files		✓				
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)			✓			
Online gaming (educational)				✓		
Online gaming (non-educational)			✓			
Online gambling			✓			
Online shopping/commerce, file sharing, use of social media, use of messaging apps, use of video broadcasting (e.g. YouTube)				✓		

8.2 Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

8.2.1 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart below for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

8.2.2 Other Incidents

It is hoped that all members of the Twynham Learning school community will be responsible users of digital technologies, who understand and follow Trust policy. However, there may be times when infringements of the policy could take place, through users being careless or irresponsible or, occasionally, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below)
- 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 or an appropriate local or national organisation
    - Police involvement and/or action

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Promotion of terrorism or extremism
- Other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed incident log form should be retained by the DSL for evidence and reference purposes**.**

8.3 Actions & Sanctions

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

Staff Incidents	Actions					Further Action
	Refer to line manager	Refer to Headteacher	Refer to Core Services HR	Refer to Police	Refer to IT Technician for action	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓	✓
Inappropriate personal use of the internet / social media / personal email	✓	✓	✓		✓	
Unauthorised downloading or uploading of files	✓		✓		✓	✓
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	✓		✓		✓	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓		✓	
Deliberate actions to breach data protection or network security rules	✓	✓	✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils	✓	✓	✓			
Actions which could compromise the staff member's professional standing	✓	✓	✓			✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓		✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓		✓		✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓

9. Remote learning

All remote learning is delivered in line with the Trust's Remote Learning Policy.

Schools, in consultation with IT technicians, will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

Schools, in consultation with IT technicians, will ensure that all Trust-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During a period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

Schools will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

10. Child-on-Child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Up skirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationships

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

Staff will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The relevant school(s) will respond to these incidents in line with the Safeguarding and Child Protection Policy and local Child Protection Procedures.

Twynham Learning schools will respond to all concerns regarding online child-on-child sexual abuse and harassment involving one or more of their pupils, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

11. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer’s attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel ‘special’, particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. Schools will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

11.1 Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding & Child Protection Policy.

12. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim’s phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else’s name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny / misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

13. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil’s mental state, both positively and negatively. Schools will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Positive impacts:

- Creates a sense of social support, connectedness and positive interaction, which can boost mental health
- Helps to foster and sustain relationships with friends and family, especially those who live far away
- Provides a way to make new friends and connections with peers who share similar interests or experiences
- Helps some young people to be more open and honest with their friends about how they think and feel
- Makes some young people feel supported and less alone during tough times, as they can read about other people’s similar experiences
- Empowers young people with disabilities or communication needs through creating a sense of community and belonging
- Helps children and young people to learn how to strengthen their mental health and keep themselves well
- Provides easier access to informal and formal support – help that is available at different times of the day

- Provides a platform on which to be creative and have fun

There are, however, potential risks that social media and the internet can have on children and young people's mental health, which may also affect their ability to thrive and achieve.

Negative impacts:

- Disrupted sleep - Children who use social media at night may not be getting enough sleep. This can not only impact on their learning at school, but a lack of sleep can also increase the risk of depression and anxiety. Children aged 5-16 need to get between 11 hours and 9 hours of sleep a night.
- Accessing harmful or inappropriate content - Children may access content that is violent, racist, hateful or features pornographic material. Studies show that the majority of children and young people are more likely to initially stumble across pornography through targeted adverts or content, rather than intentionally searching for it. When they first accessed pornography, young people were most likely to report that they felt curious, but also shocked, confused or disgusted.
- Cyberbullying - Children and young people may carry out or be exposed to bullying behaviour online. Like bullying offline, cyberbullying also increases a child's risk of developing depression and lowered self-esteem. Research has found that children and young people who experience cyberbullying are twice as likely to self-harm.
- Body image - In a survey conducted by the Mental Health Foundation, 40% of young people (26% of boys and 54% of girls) said that images on social media had made them worry in relation to their body image. Children and young people may compare themselves to celebrities, bloggers or people they are inspired by and begin to filter or manipulate images of themselves to conform to "body ideals" that are often promoted online. Body dysmorphia disorder is when a child or young person persistently worries about aspects of their body or how they look – this can have a huge impact on their life.

Click link for further information: Internet and social media : Mentally Healthy Schools