SIR JOHN THURSBY COMMUNITY COLLEGE

Online Safety Policy

Reviewed:	September 2026
Date approved by Governors:	29th September 2026
To be reviewed:	September 2027
Person Responsible:	Assistant Headteacher

AMBITION
RESPECT
BELONGING

Contents

1. Introduction

1.1 Rationale 3

1.2 Online safety requirements for schools 3

1.3 Development/Monitoring/Review of this Policy 4

1.4 Scope of the Policy 4

1.5 Links to other school policies 4

2. Roles and Responsibilities

2.1 Governors 5

2.2 Headteacher and Senior Leaders 5

2.3 Online Safety Coordinator 6

2.4 Network Manager / Technical staff 6

2.5 Teaching and Support Staff 6

2.6 Child Protection / Safeguarding Designated Person (DSL) 7

2.7 Online Safety Group 7

2.8 Students 7

2.9 Parents/Carers 8

3. Policy Statements 8

3.1 Education – students 8

3.2 Education – parents / carers 9

3.3 Education & training – Staff / Volunteers 9

3.4 Training – Governors 10

3.5 Technical – infrastructure / equipment, filtering and monitoring 10

3.6 Use of digital and video images 11

3.7 Data protection 11

3.8 Passwords 12

3.9 Mobile phones 13

3.10 Using blogs, wikis, podcasts and other mechanisms to publish content online 13

3.11 Use of social media 13

3.12 Email

3.13 Remote learning (COVID-19) Communication with students 15

4. Dealing with unsuitable / inappropriate activities 15

4.1 Unsuitable / inappropriate activities 15

4.2 Responding to incidents of misuse 18

4.2.1 Illegal incidents 18

4.2.2 Other incidents 19

4.3 Actions and Sanctions 21

5. Appendices 25

Introduction

1.1 Rationale

The school's policy has been written to ensure safety measures are in place to protect both students and staff working with ICT equipment and related technologies at SJT. The policy is to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own and students' standards and practice. Our responsibility is to set high expectations of our students using communication technologies and to maintain a consistent approach to Safeguarding by knowing the content of the policy and the procedures within this policy.

1.2 Online safety requirements for schools

The Department for Education (DfE) has published an updated version of its statutory safeguarding guidance, Keeping Children Safe in Education, which is in force from September 2026. The guidance includes enhanced information about safeguarding children online. References are made to the importance of staff training and raising the awareness of online safety and safeguarding with staff, students and parents and carers. The guidance places an emphasis on schools working in a preventative manner to proactively protect students.

In particular, (page 38) of the guidance identifies 4 key categories of risk:

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

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or 38Public Health England: has now been replaced by the UK Health Security Agency and the Office for Health Improvement and Disparities (OHID), which is part of the Department of Health and Social Care, and by the UK Health Security Agency, however branding remains unchanged. 36 financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

As a school we ensure the following:

- An appropriate filters and monitoring systems in place which are reviewed annually.
- a whole school approach to online safety (including the use of mobile technology)
- regular updated online safety training for staff
- Use of mobile devices is not allowed by students and sanctions are in place should this occur
- Students are expected to keep their phone in a sealed YONDR pouch for the duration of the school day if they need to have them in school
- Students do not have access to school Wi-Fi
- Students are educated via the assembly programme on topics such as online bullying, harassment and digital footprints
- Annual reviews of the ICT and PSHE curriculum ensures that the 4 Cs are covered to enhance student safety.
- An annual review of online safety via the KCSiE recommended Online Safety Audit Tool (360safe)

1.3 Development/Monitoring/Review of this Policy

This Online safety policy has been developed in collaboration with members of the Leadership, DSL for Child protection/Safeguarding, Online safety coordinator, staff, governors, students, parents and carers.

This Online Safety policy was approved by the Governing Body on	
The implementation of this Online Safety policy will be monitored by	Marc Smith (AHT & Online Safety Coordinator)
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents)	At least once a year
Monitoring will take place at regular intervals:	At least once a term
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2027
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA ICT manager, LA Safeguarding Officer, Police

The school will monitor the impact of the policy using: Logs of reported incidents

- Monitoring logs of internet activity (including sites visited)/filtering. CPOMS is used to record any online safety concerns, appropriate actions and outcomes.
- Internal monitoring data for network activity
- Surveys / questionnaires of students, parents / carers, staff

1.4 Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empower Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). 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 / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

1.5 Links to other school policies

a. Safeguarding

Sir John Thursby is committed to keeping students safe online. We therefore ensure that:

- ALL staff and volunteers understand that children can be harmed online via hurtful and abusive messages, enticing children to engage in age-inappropriate conversations, sharing and production of indecent images or encouraging risk taking behaviour
- The school's Online Safety Policy details how we keep students safe when using the internet and mobile technology

- Online bullying by students, via texts and emails, will be treated as seriously as any other type of bullying and will be managed through our Anti-bullying / Climate for Learning Policy
- There is a clear and explicit procedure for dealing with mobile phones that are brought into school and used by students
- DfE advice; Searching, Screening and Confiscation is followed where there is a need to search a student for a mobile device
- When school become aware of an online safety issue that has occurred outside of school, it is managed in accordance with the school Online Safety Policy. Sir John Thursby is committed to recording all matters relating to the welfare of all students and staff and uses CPOMS as its platform to record concerns, actions and outcomes

b. Other policies

This Online Safety Policy operates in conjunction with other policies including those for Student Behaviour, Anti - Bullying, Curriculum, Data Protection, plus the Home-School Agreement. There is also a policy upcoming based around the use of A.I. in schools. This will seek to cover, including, but not limited to:

- deepfakes
- AI-generated intimate images
- AI chatbots/companions
- misinformation generated by AI
- staff and student use of generative AI

2. Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school.

2.1 Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at the Online Safety Group meetings
- regular monitoring of Online Safety incident logs during the meetings
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

2.2 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 Online Safety Co-ordinator.
- The Headteacher and (at least) another member of the Leadership Team 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. (see flow chart on dealing with Online Safety incidents).
- The Headteacher and Senior Leaders are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure 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 is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Leadership Team will receive regular monitoring reports from the DSL and Online Safety Co-ordinator.

2.3 Online Safety Coordinator: Mr M Smith

- leads the Online Safety Committee
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of Online Safety incidents and creates a log of incidents through CPOMS to inform future Online Safety developments (filtering and monitoring)
- checks onGuard daily to scan for online safety issues
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Governor meetings
- reports regularly to Leadership Team

2.4 Network Manager: Mr C Camacho

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy (Cumbria and Lancashire online Network CLEO), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy" for good practice)
- that the use of the network / internet / remote access attempted misuse can be reported to the Headteacher / Senior Leader; Online Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school / academy policies (Netsweeper implemented)
- Review and implementation of any updates linked to the filtering system: Netsweeper - https://www.netsweeper.co.uk/

2.5 Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher, LT or Online Safety Coordinator for investigation / action / sanction.
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the Online Safety and acceptable use policies

- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons, where internet use is pre-planned, students 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.

2.6 Child Protection / Safeguarding Designated Person (DSL)

DSLs should 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 and misuse of artificial intelligence, including the creation, sharing or possession of AI-generated harmful content
- AI-generated intimate images, deepfakes and synthetic media which may constitute child-on-child abuse, sexual harassment or image-based abuse
- Misinformation, disinformation and conspiracy-based content which may increase vulnerability to radicalisation, exploitation or other safeguarding risks
- Online impersonation, coercion or exploitation facilitated through AI tools, chatbots or other emerging technologies
- Ensuring that safeguarding responses to online harms remain effective as technologies evolve and new risks emerge

2.7 Online Safety Committee

The Online Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. The committee is to be also responsible for regular reporting to the Governing Body.

Members of the Online Safety Committee will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety policy / documents
- the production / review / monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the Online Safety provision
- monitoring improvement actions identified through use of the 360-degree safe self- review tool
- Completing tasks and taking responsibility of actions linked to the 4 Cs as outlines in KCSiE 2026

2.8 Students

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- 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 / 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 school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

2.9 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local Online Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and online student records
- their children's personal devices in the school

3. Policy Statements

3.1 Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people need the help and support of the 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 provided as part of ICT & Computing lessons reviewed annually
- Key Online Safety messages reinforced as part of a planned programme of assemblies and form activities
- Students taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students will be taught to identify and critically evaluate AI-generated content, including deepfakes, manipulated images, synthetic media and misinformation.
- Students will be educated about the risks associated with generative AI, including online scams, image-based abuse, harmful influencers, radicalising content and the spread of false information.
- Students will develop the skills to verify sources, challenge misinformation and understand how algorithms and AI tools can influence online behaviour and decision making.
- Students taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students encouraged to adopt safe and responsible use both within and outside school
- Staff to act as good role models in their use of digital technologies, the internet and mobile devices
- Students to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Students will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.

- Students should understand 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.
- In lessons where internet use is pre-planned, it is best practice that students are 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 students are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit and report any concerns to the online safety coordinator.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that those sites are temporarily removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and approved by the Online Safety Coordinator.

3.2 Education – parents / carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. 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.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications (see appendix for further links / resources)
- Ensure that up to date guidance, advice and links for parental support is available on the school website
- ClassCharts

3.3 Education & Training – Staff / Volunteers

It is essential that all staff, including volunteers, 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 annually via the Child Protection training. 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 should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements
- The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisation
- 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 will provide advice / guidance / training to individuals as required.
- An annual questionnaire is sent to staff to identify Online safety training completed and any online safety training required. Staff are encouraged and expected to raise this training as a CPD request via their annual appraisal.

3.4 Training – Governors

Governors should take part in Online Safety training and awareness sessions, with particular importance for those who are members of any online safety committee by:

Participation in online training

Discussion and information sharing during the online safety committee meetings

Attending information sessions for staff or parents

3.5 Technical – infrastructure / equipment, filtering and monitoring

- School technical requirements are aligned and underpinned with the 'Meeting digital and technology standards in schools and colleges' policy from the DfE (Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK (www.gov.uk)
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices and will be provided with a username and secure password. Users are responsible for the security of their username and password
- The network manager is responsible for ensuring that software licence logs are accurate and up to date
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband via CEO using Netsweeper managed by LCC and onGuard. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Internet filtering will ensure that children are safe from terrorist and extremist material when accessing the internet.
- Safeguarding alerts generated through Netsweeper and onGuard are reviewed daily during term time by nominated safeguarding staff. Urgent alerts are escalated immediately to a DSL and recorded on CPOMS.
- The effectiveness of the school's filtering and monitoring systems will be formally reviewed at least annually.
    - The review will:
        - be led by the Online Safety Coordinator, DSL and Network Manager;
        - include the responsible governor for online safety;
        - evaluate whether systems are effective in identifying and managing safeguarding risks;
        - consider emerging online risks including artificial intelligence, deepfakes, harmful influencers, misinformation and online exploitation;
        - review trends from Netsweeper reports, CPOMS records and safeguarding incidents;
        - identify required actions, improvements or changes to filtering categories and monitoring arrangements;
        - be documented and reported to governors as part of the annual online safety review process.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. Monitoring is carried out
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Online Safety co-ordinator
- Appropriate security measures are in place through the facilities management provider to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices

- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

3.6 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying 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 school 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 students 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 eg on social networking sites.
- 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 students 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, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (may be covered as part of the AUA signed by parents or carers at the start of the year
- Student's work can only be published with the permission of the student and parents or carers
- Use of AI in school is solely through Copilot which is provided by Microsoft office. No other AI system should be used when incorporating any student data

3.7 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary

- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It complies with a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.
- No student data is used in A.I. programmes other than Copilot, existing rules surrounding GDPR still apply

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
- 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.

3.8 Passwords

- A secure and robust username and password convention exists for all system access. (Email, network access, school management information system)
- All information systems require staff to change their password at first log on. Where appropriate students will be assisted by members of staff in this particular task
- Staff should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised
- Staff should change their passwords whenever there is any indication of possible system or password compromise
- Student's passwords will be managed by the appropriate member of support/teaching staff and changed when is deemed appropriate
- All staff have a responsibility for the security of their username and password. Staff 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. Staff are expected to comply with the following password rules;
    - Do not write down any passwords

- Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
- Always use your own personal passwords to access computer-based services, never share these with other users.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Never save system-based usernames and passwords within an internet browser
- Staff/Governors who are looking to access the school network outside of the school WIFI zone must use two factor authentication to protect access.

3.9 Mobile phones

Students should follow the relevant school rules if they decide to bring their mobile phone or personally owned device into school. Students must place their device in a sealed YONDR for the duration of the school day. As a school we recommend that students do not bring their personal device into school.

Staff use of mobile devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity
- Certain identified staff will be issued with a school phone where contact with students, parents or carers is required
- Mobile phones and personally owned devices will be stored securely with personal belongings within school and not used in school other than in the staff lounge and staff workroom by the pigeonholes at breaktime and lunchtime
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work provided equipment for this purpose

3.10 Using blogs, wikis, podcasts and other mechanisms to publish content online

- Blogging, podcasting and other publishing of online content by students will take place within the school learning platform or school website
- Students will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff
- Any public blogs run by staff on behalf of the school will be hosted on the learning platform/school website/blog and postings should be approved by the head teacher before publishing
- Staff will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, students will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

3.11 Use of social media

- See school Social Media policy – adopted LCC policy

3.12 Email

Staff should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

- Where possible access to personal email accounts should be restricted to non-contact time and should be kept to a minimum.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Access, in school, to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and productivity and will be restricted in line with the school Acceptable Use Policy.
- The school gives all appropriate staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- School email accounts should be the only account that is used for school-related business.
- Staff will only use official school-provided email accounts to communicate with students and parents and carers, as approved by the leadership team.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.
- Irrespective of how staff access their school email (from home or within school), school policies still apply.
- Emails sent to external organisations should be written carefully and, where necessary, authorised before sending to protect the member of staff sending the email.
- Chain messages will not be permitted or forwarded on to other school-owned email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school'.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations, parents or students, are advised to carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence.
- When away for extended periods, 'out-of-office' notification should be activated so that colleagues are aware that you are not currently available.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies need to be controlled and never communicated through the use of a personal account
- Staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All email and email attachments will be scanned for malicious content.
- Staff should never open attachments from an untrusted source but should consult the network manager first.
- Communication between staff and students or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All email users within school should report any inappropriate or offensive emails through the incident-reporting mechanism within school.

- Students must immediately tell a designated member of staff if they receive any inappropriate or offensive email.
- Students must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Students will be allocated an individual email account for their own use in school or class.
- Students may only use school-provided email accounts for school purposes.
- Whole class or group email addresses will be used in school for communication outside of the school.
- Students may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Students and staff will be reminded when using email about the need to send polite and responsible messages.
- Students and staff will be reminded about the dangers of revealing personal information within email conversations.
- Students must not reveal personal details of themselves or others in email communications.
- Students should get prior permission from an adult if they arrange to meet with anyone through an email conversation.

3.13 Remote learning and Communication with students

If remote learning is needed for students

- Students will be placed into groups on Teams.
- Work will be set on Teams.
- Another member of staff (your Learning Leader, your Leadership Line Manager or the teacher who shares the group with you) will be copied into this group
- Staff will communicate with students through Teams. If staff need to communicate with individual students, they must use their school email account and copy another member of staff into the communication. Staff must not use their personal email accounts or those of the students to communicate.
- Staff should not give out any other contact details to students.
- Staff will continue to follow our safeguarding protocols in terms of social media and not engage with any students on any social media platforms.

Vulnerable Students and Families

There are a limited number of staff involved in communicating with our vulnerable students and families during a closure or during the school day. These staff should ensure that any communication is uploaded to CPOMS and that any messages sent directly to a student are copied to another member of the team involved or to their parent, preferably by setting up a WhatsApp or text group. Staff should not sustain any communication on a 1:1 basis with students, without another member of staff or the student's parents being copied into the messages. Only staff with elevated safeguarding and attendance-based communication will communicate with parents and carers using WhatsApp messenger.

4. Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school 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 may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

4.1 Unsuitable / inappropriate activities

The school 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 school policy restricts usage as follows:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	Pornography				X	
	Promotion of any kind of discrimination threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
Using any A.I. tool other than Copilot with any school data				X	
Online gaming (educational)		X			
Online gaming (non-educational)				X	
Online gambling				X	
Online shopping / commerce				X	
File sharing			X		
Use of social media				X	
Use of messaging apps (unless identified as stated on Page 17)				X	
Use of video broadcasting e.g. Youtube		X			

All incidents whereby a student is deemed to have searched an inappropriate term or phrase is considered by the Online Safety Coordinator, who is also a DSL. Daily reports are monitored and appropriate action occurs if there is a concern.

All searches that require investigation are recorded on CPOMS. Depending upon the severity of the search either a pastoral member of staff or DSL will speak with the student. The outcome of that discussion will vary depending on the search and the reason for the search. There are occasions that inappropriate searches are flagged where the intention is linked to education.

Where there is concern or evidence of intent, appropriate sanctions and / or educational conversations will occur and where appropriate parents /carers will be informed.

Where the concern is repeat and is linked to discrimination, appropriate sanctions will be issued alongside educational work.

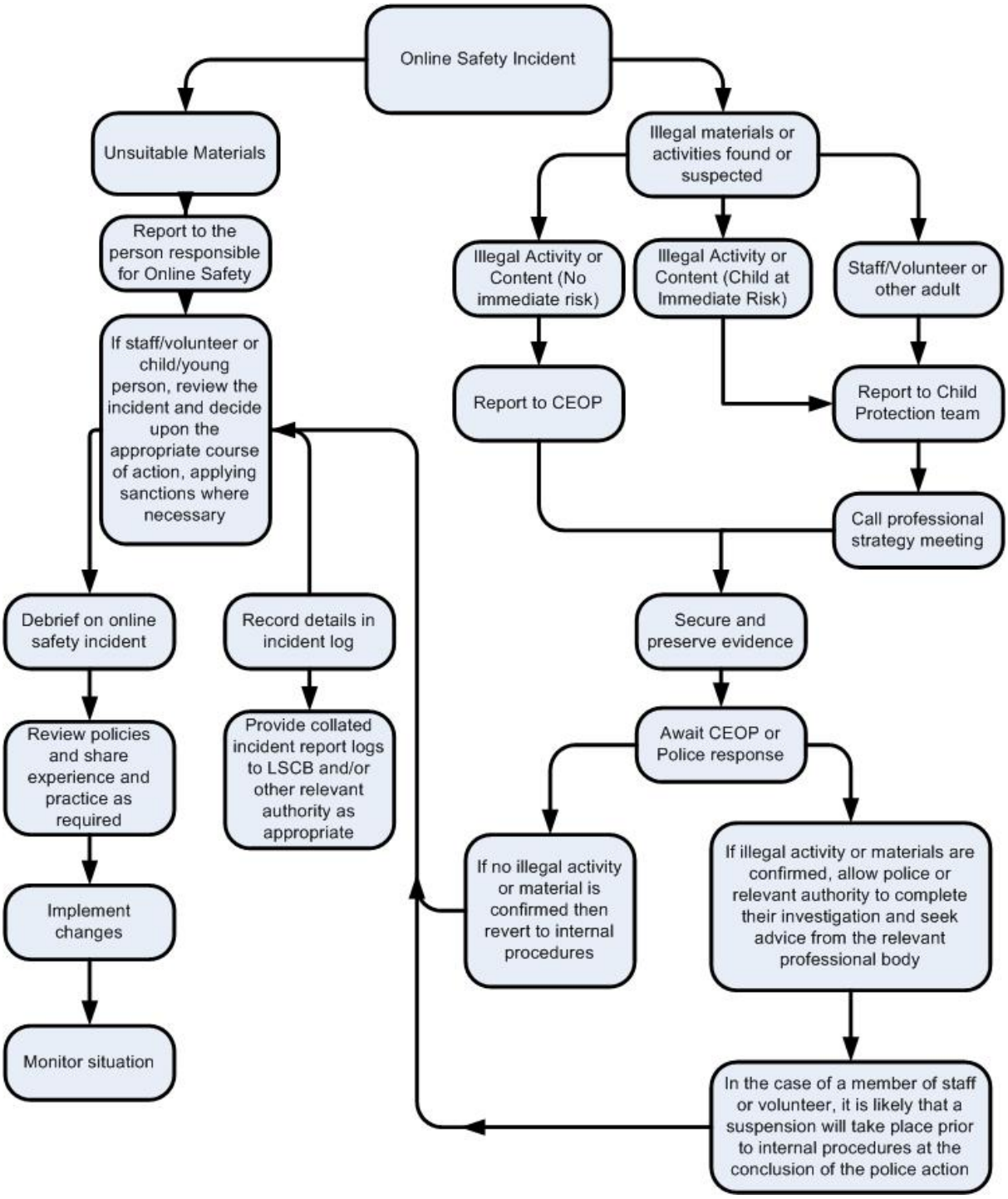
Our Internal Alternate Provision (The Bridge) and Repair Room work to deliver personalised education sessions around issues that arise.

Whereby the searches and comments are linked to extremist views the Online Safety coordinator will consider a Channel Referral.

4.2 Responding to incidents of misuse

4.2.1 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 and appendix) for responding to online safety incidents and report immediately to the police.



4.2.1 Other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, 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 Local Authority / Academy Group or national / local organisation (as relevant).
    - 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 for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

For incidents where searches and internet use are inappropriate, but not illegal the following protocol is used by staff. All searches of inappropriate content are identified by the Netsweeper or onGuard filtering system and reported on a daily and weekly basis.

ONLINE SAFETY PROTOCOL

NETWORK MONITORING AND PROTECTION

✓ Network filtering blocks suspicious searches.
✓ Daily safeguarding reports are reviewed.
✓ Searches linked to radicalisation, discrimination, pornography, aggression and terrorism are monitored.
✓ onGuard alerts provide real-time monitoring of school systems.
✓ Students receive education, support and protection where concerns arise.
✓ Referrals to external agencies are made where necessary.
✓ Staff should never knowingly view or search for a suspected indecent image, this must be reported directly to a DSL. Staff who accidentally view an image should always inform a DSL.

REPORTING ONLINE SAFETY CONCERNS

Online grooming or exploitation
Sexting
Sharing indecent images
Cyberbullying
Inappropriate online searches
Misuse of Generative AI

IMMEDIATE ACTION REQUIRED

NON-URGENT CONCERN	URGENT CONCERN
Speak to the Year Team Record on CPOMS (CIA) Follow Year Team advice	Contact a DSL immediately Same-day safeguarding response required Escalate the concern immediately

DESIGNATED SAFEGUARDING LEADS (DSLs)

Name	Role
Nikki Tregay	Assistant Headteacher
Kate Tempest	Family Support Manager
Andrew Harwood	Deputy Headteacher
Marc Smith	Assistant Headteacher
Matt Renshaw	Headteacher

OUTCOMES AND RESPONSES

Concern Type	School Response
Grooming / Exploitation	Parents informed. Appropriate referral completed. Police informed where appropriate.
Sexting	Parents informed and appropriate support provided.
Sharing Indecent Images (Child)	Seize device. Contact parents and police.
Cyberbullying	Year Team support. School investigation and response.
Inappropriate Searches or Misuse of AI	Educational intervention, parental contact and follow-up action.

IMPORTANT SAFEGUARDING MESSAGE

All internal concerns will result in a school investigation to support and safeguard the students involved. Police and/or other appropriate agencies will be informed where activity is believed to be illegal. Advice from CEOP will be sought where necessary.

C = Concern | I = Information / Intervention | A = Action

4.3 Actions and Sanctions

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. The following is designed as a guide and actions may be taken in response to specific circumstances. All serious incidents would be investigated and we take a proportionate, transparent and measured approach:

Students Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X		
Unauthorised use of non-educational sites during lessons	X				X				
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X							
Unauthorised / inappropriate use of social media / messaging apps / personal email	x				x		x	x	
Unauthorised downloading or uploading of files	x				x		x	x	
Allowing others to access school network by sharing username and passwords	x				x		x	x	
Attempting to access or accessing the school network, using another student's / pupil's account	x				x		x	x	
Attempting to access or accessing the school network, using the account of a member of staff			x		x	x	x		x
Corrupting or destroying the data of other users			x		x	x	x		x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x			x	x	x		x
Continued infringements of the above, following previous warnings or sanctions		x	x		x	x	x		x

Students Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year /	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access	Warning	Further sanction eg detention / exclusion
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x		x	x	x		x
Using proxy sites or other means to subvert the school's filtering system		x	x		x	x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	x	X		
Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x	x	x		x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x							x	
Misuse of A.I. including but not limited to: • AI-generated images • Deepfakes • "Nudification" apps that create sexualised images from ordinary photographs • Generative AI misuse for bullying, harassment and misinformation	X	X	X	X	X	X	X	X	X
Searching for, accessing or sharing areas that may lead to online risk, including, but not limited to: • misinformation • disinformation • conspiracy theories • online radicalisation • misogynistic content • harmful influencers	X	X	X	X	X	X	X	X	X

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	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	X	x			x
Inappropriate personal use of the internet / social media / personal email	x	x			x	x		
Unauthorised downloading or uploading of files	x				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	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner		x			x	x		
Deliberate actions to breach data protection or network security rules		x	x		x	x	x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x				x	x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x			x	x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	x	x	x			x		
Actions which could compromise the staff member's professional standing	x	x	x			x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x			x	x	x
Using proxy sites or other means to subvert the school's / academy's filtering system		x			x	x		x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x		x	x		
Deliberately accessing or trying to access offensive or pornographic material		x	x		x		x	x
Breaching copyright or licensing regulations	x					x		
Misuse of A.I. including but not limited to: • AI-generated images • Using non-approved A.I. programmes	X	X	X	X	X			X
Continued infringements of the above, following previous warnings or sanctions		x	x				x	x

Appendices

1. **ICT Security Framework including;**

    a. **Student Acceptable Use and Good Practice rules – for students**
    b. **Staff (and Volunteer) Acceptable Use Policy Agreement**
    c. **Acceptable Use Agreement for Community Users**

2. **Online Safety Committee Terms of Reference**

3. **Legislation**

Staff

School ICT, Internet, Email and AI Acceptable Use & Good Practice

September 2026

AMBITION	RESPECT	BELONGING
Use technology to work, create and improve.	*Protect people, privacy and their work.*	*Be professional, inclusive and report concerns.*

The school provides access to ICT systems, including computers, email, cloud services, and the internet, to support teaching, learning, administration and school business. These rules are designed to keep staff and students safe, ensure systems remain secure, and promote responsible, professional and ethical use of technology, including artificial intelligence (AI).

1. Responsible and Appropriate Use

- ICT systems must only be used for teaching, learning, administration, school business, or other approved professional purposes.
- Use of the school network must always support the work of the school and be appropriate to education.
- Limited personal use is only permitted where it does not interfere with work, safeguarding, security, or the school's reputation.

2. Accounts, Security and Access

- Staff must only use their own authorised login and must keep passwords, authentication codes, and security tokens secure and private.
- Staff must not attempt to bypass or disable security systems such as filtering, monitoring, device management, or file restrictions.
- The use of proxies, VPNs, or other tools to bypass filtering or monitoring systems is strictly prohibited unless an approved technical procedure has been followed.
- Staff must not attempt to gain unauthorised access to systems, networks, accounts, or data.
- Multi-Factor Authentication (MFA) must be used where required.
- Devices must be locked when unattended and signed out when work is complete.
- Any suspected account compromise, phishing, malware, or unusual sign-in activity must be reported to IT immediately.

3. Files, Storage and Equipment

- Staff must only access, change, delete, or share files required for their authorised duties.
- Work must be saved securely in approved school locations.
- Personal email, consumer file-sharing services, and unapproved storage services must not be used for school information.
- Unauthorised removable storage devices, software, browser extensions, hardware, or applications must not be used.
- School devices must not be shared with family or friends.
- Any loss, theft, damage, or security concern involving school equipment must be reported immediately.

4. Internet and Online Safety

- Internet access must be used responsibly and professionally.
- Use of unauthorised social networking sites, chat rooms, or other online services for school business is not allowed.
- Staff must use approved school communication channels when contacting students and families and must maintain appropriate professional boundaries.
- Illegal, harmful, offensive, discriminatory, misleading, or otherwise inappropriate content must not be accessed, created, requested, stored, linked to, sent, or shared.
- Any inappropriate, harmful, or concerning content must be reported immediately to the Designated Safeguarding Lead and to IT where relevant.
- Staff must not personally investigate suspected illegal or safeguarding material and must avoid unnecessary viewing, copying, forwarding, or deletion.

5. Email and Communication

- All communication must be accurate, polite, appropriate, professional, and responsible.
- School accounts must be used when communicating with students, families, colleagues, or external organisations about school business.
- Personal email accounts, personal social media accounts, and private messaging services must not be used for professional contact unless an approved procedure specifically allows it.
- Emails and messages should be treated as potentially public, as they may be forwarded or disclosed.
- Anonymous messages, chain letters, spam, or inappropriate communication must not be sent.
- Recipients, attachments, links, and sharing permissions must be checked before sending information.

6. Copyright and Data Protection

- Copyright, software licensing, intellectual property, and the work of others must always be respected.
- Personal, special category, safeguarding, and confidential information must only be accessed, stored, shared, or uploaded for an authorised purpose using approved systems.
- Only the minimum information required for the task should be used.
- Confidential information about students, staff, families, or the school must not be disclosed unless authorised and there is a lawful professional need.
- Any actual or suspected personal data breach must be reported immediately through the school's reporting process.

7. Use of Artificial Intelligence (AI)

The school recognises that AI can support teaching, learning, administration and school business when used appropriately, but strict rules apply:

7.1 Acceptable Use of AI

- Only AI tools approved by the school may be used for school business.
- AI may be used to support planning, drafting, research, idea generation, and understanding, but it must not replace professional judgement or accountability.

7.2 Professional Responsibility

- Staff remain responsible for checking the accuracy, quality, bias, provenance, copyright, safeguarding implications, and suitability of AI outputs.
- AI-generated content must not be presented as verified fact or as professional judgement without appropriate review.
- AI must not be used to make high-impact decisions about students or staff without authorised human oversight.

7.3 Safe and Ethical AI Use

- AI tools must not be used to create harmful, misleading, discriminatory, deceptive, or inappropriate content.
- AI must not be used to imitate a real person or create fake or manipulated images, video, or audio without an authorised and lawful purpose.

7.4 Data Protection and Privacy

- Personal data about students or staff, confidential safeguarding information, assessment data, credentials, or sensitive school information must never be entered into public or unvetted AI systems.

- AI interactions within school systems may be monitored for safeguarding, security, and compliance purposes.

8. Personal and Work Mobile Phones

- Staff must not carry or use a personal mobile phone in student spaces during the working day.
- The only exception is for a member of staff who has been provided with a school-issued work mobile phone. The work phone may be carried and used for authorised school duties.
- Personal phones must be stored securely away from student spaces and must not be used to photograph, record, communicate with, or process information about students.
- Any use of a school-issued work phone must follow this policy, safeguarding requirements, and data protection rules.

9. Monitoring and Safeguarding

- The school may monitor usage of ICT systems, including websites, email, messages, accounts, and files, to ensure safety, security, and compliance.
- Monitoring may include reviewing content, intercepting communications, and removing inappropriate material where necessary.
- Staff must know how to report a failure or concern involving filtering and monitoring and must ensure students in their care follow the Student Acceptable Use Policy.

10. Reporting Concerns

- Any concerns about inappropriate use, unsafe content, safeguarding, data protection, cyber security, or misuse of ICT or AI must be reported immediately through the relevant school process.
- Safeguarding concerns must be escalated immediately to the Designated Safeguarding Lead.
- Staff must preserve relevant evidence without unnecessarily accessing, copying, or distributing harmful material.

11. Consequences of Misuse

- Failure to follow these rules may result in loss of access to ICT systems and further action under the Staff Code of Conduct, disciplinary procedures, contractual arrangements, or other relevant school policy.
- Serious breaches, including misuse of AI, personal data, safeguarding information, or attempts to compromise security, may be referred to professional bodies, regulators, safeguarding partners, or the police where appropriate.

Student

School ICT, Internet, Email and AI Acceptable Use & Good Practice

September 2026

AMBITION	RESPECT	BELONGING
Use technology to learn, create and improve.	Protect people, privacy and their work.	Be kind, include others and report concerns.

The school provides access to ICT systems, including computers, email, cloud services, and the internet, to support learning and education. These rules are designed to keep all students safe, ensure systems remain secure, and promote responsible and ethical use of technology, including artificial intelligence (AI).

1. Responsible and Appropriate Use

- ICT systems must only be used for schoolwork, homework, or approved educational purposes unless permission is given by a member of staff.
- Use of the school network must always support learning and be appropriate to education.

2. Accounts, Security and Access

- Students must only use their own authorised login and must keep passwords secure and private.
- Access to systems must not be shared with anyone else.
- Students must not attempt to bypass or disable security systems such as filtering, monitoring, or file restrictions.
- The use of proxies, VPNs, or other tools to bypass filtering or monitoring systems is strictly prohibited.
- Students must not attempt to hack, disrupt, or gain unauthorised access to systems, networks, or data.
- The security of ICT systems must not be compromised under any circumstances.
- When accessing school Microsoft accounts from home, Multi-Factor Authentication (MFA) must be used.

3. Files, Storage and Equipment

- Students must not access, change, delete, or interfere with other users' files.
- Work should be saved securely in personal areas, not shared spaces.
- Files stored in shared locations may be removed by the school.
- Students must not bring in or use removable storage devices (such as USB drives or external hard drives).
- Electronic files must not be brought into school without permission.
- Any damage to ICT equipment may result in sanctions and charges for repair.

4. Internet and Online Safety

- Students must ask permission before accessing websites unless directed by a teacher.
- Use of chat rooms and unauthorised social networking sites is not allowed.
- Students must not sign up to personal websites using their school email address.
- Personal information (such as address, phone number, or meeting arrangements) must never be shared online.
- Any inappropriate, harmful, or concerning content must be reported immediately to a member of staff.

5. Email Use

- Emails must only be sent to known or approved contacts.
- All communication must be polite, appropriate, and responsible.
- Emails should be treated as public, as messages may be forwarded.
- Anonymous messages, chain letters, or inappropriate communication must not be sent.
- Emails to staff must be school-related, respectful, and sent within reasonable hours (8:00am–6:00pm).

6. Copyright and Data Protection

- Students must not download or store copyrighted material without permission.
- Intellectual property and the work of others must always be respected.
- Personal or sensitive information must not be stored, shared, or uploaded without permission.
- Students must never input personal data (their own or others') into AI tools.

7. Use of Artificial Intelligence (AI)

The school recognises that AI can support learning when used appropriately, but strict rules apply:

7.1 Acceptable Use of AI

- AI tools may be used to support learning, such as research, idea generation, and understanding concepts.
- Students must understand that AI is a tool to assist learning, not replace it.

7.2 Academic Integrity

- All academic work must be the student's own original work.
- AI must not be used to generate coursework, essays, or assignments.
- Any permitted use of AI must be declared where required.

7.3 Safe and Ethical AI Use

- AI tools must not be used to create harmful, misleading, or inappropriate content.
- Students must understand risks such as misinformation, bias, and deepfakes.
- AI outputs must not be blindly trusted and should always be checked.

7.4 Data Protection and Privacy

- Personal, sensitive, or identifiable information must never be entered into AI systems.
- AI interactions within school systems may be monitored for safeguarding and compliance purposes.

8. Monitoring and Safeguarding

- The school may monitor usage of ICT systems, including websites, emails, and files, to ensure safety and compliance.
- Monitoring may include reviewing content, intercepting communications, and removing inappropriate material where necessary.

9. Reporting Concerns

- Any concerns about inappropriate use, unsafe content, or misuse of ICT or AI must be reported immediately to a member of staff.

10. Consequences of Misuse

- Failure to follow these rules may result in loss of access to ICT systems and further disciplinary action.
- Serious breaches, including misuse of AI or attempts to compromise security, may result in further sanctions in line with school policy.

Appendix 2 - Online Safety Committee Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives.

2. Membership

2.1. The online safety committee will seek to include representation from all stakeholders.

The composition of the group should include:

- LT member/s
- DSL
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent / Carer
- ICT Technical Support staff (where possible)
- *Student / pupil representation* – for advice and feedback. *Student / pupil voice is essential in the make-up of the online safety group, but students / pupils would only be expected to take part in committee meetings where deemed relevant.*

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held **termly**. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
    - Staff meetings
    - Student / pupil forums (for advice and feedback)
    - Governors' meetings
    - Surveys/questionnaires for students / pupils, parents / carers and staff
    - Parents evenings
    - Website/VLE/Newsletters
    - Online safety events
    - Internet Safety Day (annually held on the second Tuesday in February)
    - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Sir John Thursby Community School have been agreed

Signed by (LT): M. Smith

Date: 15/09/2026

Date for review: September 2027

Appendix 3– Legislation

Sir John Thursby Community College recognises that online safety, safeguarding and the use of digital technologies are supported by a range of legislation and statutory guidance. This policy should be read alongside the legislation and guidance outlined below.

1. Keeping Children Safe in Education (KCSIE) 2026
Keeping Children Safe in Education (KCSIE) 2026 is the Department for Education statutory safeguarding guidance for schools and colleges in England. Online safety is recognised as an integral part of safeguarding and schools are expected to adopt a whole-school approach to protecting children both online and offline.

2. Online Safety Act 2023
The Online Safety Act 2023 places duties on providers of regulated online services to assess and mitigate risks from illegal content and content harmful to children, strengthening protections for children online.

3. Data Protection Act 2018 and UK GDPR
The Data Protection Act 2018 and UK GDPR govern how personal information is collected, stored, processed and shared.

4. Computer Misuse Act 1990
Creates offences relating to unauthorised access to computer material and acts which impair computer systems.

5. Communications Act 2003
Contains offences relating to grossly offensive, indecent, obscene or menacing electronic communications.

6. Malicious Communications Act 1988
Creates offences relating to electronic communications conveying threats, false information or intended to cause distress or anxiety.

7. Protection from Harassment Act 1997
Applies to offline and online behaviour including cyberbullying, stalking and harassment.

8. Sexual Offences Act 2003
Includes offences relating to online grooming, sexual communication with children, sexual exploitation and abuse of trust.

9. Serious Crime Act 2015
Introduced offences and safeguarding measures relating to child exploitation and communication with children for sexual purposes.

10. Counterterrorism and Security Act 2015
Places a duty on schools to have due regard to preventing people from being drawn into terrorism (Prevent Duty).

11. Education and Inspections Act 2006

Provides schools with powers to address inappropriate behaviour outside school where there is a sufficient connection to the school.

12. Protection of Freedoms Act 2012
Provides safeguards concerning biometric information and parental consent requirements.

13. Freedom of Information Act 2000
Gives individuals rights to request access to information held by public authorities.

14. Copyright, Designs and Patents Act 1988
Protects intellectual property rights and applies to digital content and resources.

15. Voyeurism (Offences) Act 2019
Relevant to image-based abuse, deepfakes and AI-generated intimate imagery.

Additional Guidance
Keeping Children Safe in Education 2026
Working Together to Safeguard Children
Searching, Screening and Confiscation (DfE)
Meeting Digital and Technology Standards for Schools and Colleges
Information Commissioner guidance
UK Safer Internet Centre guidance
Prevent Duty Guidance

Appendix 4 - Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self review tool: www.360data.org.uk

Bullying / Online-bullying / Sexting / Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

UKSIC – Appropriate Filtering and Monitoring

Somerset - Questions for Technical Support

NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom –Media Literacy Research