THE JUBILEE ACADEMY

Aspire and Achieve

Title:	Online Safety Policy
Date Approved:	December 2021
Date Reviewed:	September 2022
Status:	Non-Statutory
Delegation:	Head of School
Responsibility:	SBM H&S and IT Technician
Review Frequency:	Annually/as required
Policy Locations:	Website/Staff Shared Drive/Hard Copy
Next Review Date:	September 2023

Online Safety Policy

Scope

This Online Safety Policy outlines the commitment of The Jubilee Academy to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Policy is intended to help all understand that **everyone** has a statutory responsibility with respect to online safety, identifying concerns, sharing information and taking prompt action when ensuring students and families are to receive the right help at the right time.

This policy applies to all members of The Jubilee Academy community (including staff, students, volunteers, parents/carers, governors, visitors or external agencies) who have access to and are users of school digital technology systems, both in and out of The Jubilee Academy

The Jubilee Academy 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.

Aims

The Jubilee Academy aims to:

- Have robust processes in place to ensure the online safety of staff, students, volunteers, parents/carers, governors, visitors or external agencies
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk (4C's)

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Policy Development, monitoring and review

This Online Safety policy has been developed by the Online Safety Group (OSG) made up of:

- Head of School
- Nominated School Governor for Safeguarding, Health & Safety, Pupil premium and SEN
- Deputy Headteacher Personal Development & Welfare who is also the Nominated School Designated Safeguarding Lead and Online Safety Lead
- School Business Manager – H&S (ICT)
- ICT Technician and Researcher
- Nominated Parent Governor
- Student Voice representation – for advice and feedback. Student/pupil voice is essential in the makeup of the online safety committee, but students/pupils would only be expected to take part in committee meetings were deemed relevant.

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule of development, monitoring and review

This online safety policy was approved by The Governing Body	*Insert date*
The implementation of this online safety policy will be monitored by the:	Online Safety Group
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the online safety policy generated by the SBM (which will include anonymous details of online safety incidents) at regular intervals:	Annually
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.	Annually / as required
Should serious online safety incidents take place, the following external persons/agencies should be informed:	**Golden Number (020 8901 2690)** Emergency Duty Team (operates out of hours): **020 8424 0999** between 5pm and 9am, Monday to Friday, 24 hours during weekends and all bank holidays. **Local Authority Designated Officer for Allegation against staff (LADO)** Initial referrals via MASH/Golden Number **(Name: Rosalind Miller)** Quality Assurance and Service Improvement, Harrow Peoples Services (**07871 987254)** **Police** **Data Protection Officer**: Judicium Consulting Limited Address: 72 Cannon Street, London, EC4N 6AE

	Email: dataservices@judicium.com Web: www.judiciumeducation.co.uk Telephone: 0203 326 9174 Lead Contact: Craig Stilwell **ICO** https://ico.org.uk/for-organisations/report-a-breach/ 0303 123 1113

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - Students
    - Staff
    - Parents/carers

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

A list of the legislative frameworks considered can be found in appendix 9

Policy and leadership

Responsibilities

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

The Governing body

The Governing body is responsible for approving this policy, for reviewing the effectiveness of the policy. holding and holding the Head of School to account for its implementation.

The Governing Body will ensure the school has appropriate filters and monitoring systems in place, and regularly review their effectiveness.

The Governing Body will that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified

The Governing board will co-ordinate regular meetings and monitor online safety logs as provided by the OSG.

The Nominated School Governor for Safeguarding, Health & Safety, Pupil premium and SEN will oversee online safety through Termly meetings with the OSG.

The role of the Safeguarding, Health & Safety, Pupil premium and SEN will include:

- regular meetings with the Online Safety Lead and SBM H&S (ICT)
- membership of the school Online Safety Group
- checking that provision outlined in the Online Safety Policy (e.g. online safety)
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors body

All governors will:

- Ensure that they have read and understood this policy and that it is renewed as required
- Agree and adhere to the terms on acceptable use of the school's ICT systems and related technologies.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.
- Procedures are in place for dealing with breaches of online-safety and security;
- The Business Continuity plan links to this policy and offers strategic direction for cyber threats
- All staff and volunteers have access to appropriate ICT training.

The Head of School

- The Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Head of School 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 Lead.
- The Head of School and Designated Safeguarding Lead 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.
- The Head of School is responsible for nominating an Online Safety Lead and ensuring they 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 Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.
- All staff should be included in online safety training. Staff must also understand that misuse of the internet may lead to disciplinary action (as detailed in section 5 of the HR Policies) and possible dismissal;
- All temporary staff and volunteers are made aware of the school's Online Safety Policy and arrangements;
- A commitment to one line Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

Designated Safeguarding Lead (DSL) and Online Safety Lead will ensure that:

Details of the school's DSL and deputy are set out in our Safeguarding including child protection training policy as well as relevant job descriptions.

The DSL 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 on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying
- Harmful sexual behaviours inc. sexual harassment and violence and online sexual abuse
- Access to extremist material
-

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Developing an online safety culture throughout the setting as part of safeguarding, which is in line with national best practice recommendations (e.g. Ofsted, DfE)
- Acting as a named point of contact on all Online Safety issues and liaising with other members of staff as appropriate
- Keeping up to date with current research, legislation and trends. This may include accessing appropriate training and using a range of approaches to enable them to understand the role of new technology as part of modern British society and the wider safeguarding agenda.
- Leading the OSG with input from all stakeholder groups.
- Working with the SBM H&S (ICT) and OSG to review and update the Online Safety policy and associated policies and agreements on a regular basis (at least annually) with stakeholder input and ensuring that Online Safety is integrated with other appropriate school policies and procedures.
- Ensuring that there is an age and ability appropriate Online Safety curriculum that is embedded, progressive, flexible and relevant which engages children's' interest and promotes their ability to use technology responsibly and to keep themselves and others safe online.
- Ensuring that the setting participates in local and national events to promote positive online behaviour, e.g. Safer Internet Day
- Ensuring that Online Safety is promoted to parents and carers and the wider community through a variety of channels and approaches
- To ensure that age-appropriate filtering is in place, which is actively monitored
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices
- Work with the lead for data protection and data security to ensure that practice is in line with legislation
- Working with the Head of School, School Business Manager H&S (SBM H&S (ICT)), ICT Technician and other staff, as necessary, to address any online safety issues or incidents
- Managing **ALL** online safety issues and incidents in line with the school's safeguarding including child protection training policy
- Ensuring that **ALL** online safety incidents are logged (see appendix 8) and dealt with appropriately in line with this policy
- Ensuring that **ALL** incidents of cyber-bullying and harmful sexual behaviours inc. sexual violence and/or harassment are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (at least annually and as part of induction) and in line with the self-audit for staff on online safety training needs (see appendix 5)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of School, Senior Leadership Team, Governing body and other agencies as appropriate

The SBM H&S (ICT) with support from The ICT Technician are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and is not open to misuse or malicious attack; and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- That users may only access the networks and devices through a properly enforced password protection policy
- Ensuring that any online safety incidents are logged (see appendix 8) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying and harmful sexual behaviours are dealt with appropriately in line with the school behaviour policy

All staff and volunteers are responsible for:

- Ensuring they have an up-to-date awareness of online safety matters and of the current online safety policy and practices
- Ensuring they have read, understood and signed the appropriate staff ICT acceptable user agreement (AUA) and adhere to the terms (see appendix 1) and Safe Working Practice Agreement- Safeguarding Students and Young People (see appendix 4)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 8) and dealt with appropriately in line with this policy
- Ensuring all digital communications with students /parents/carers should be on a professional level and only carried out using official school systems
- Ensuring online safety issues are embedded in all aspects of the curriculum and other activities
- Ensuring students understand and follow the Online Safety Policy and follow the school's terms on acceptable use (see appendix 2)
- Ensuring students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Ensuring they monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies regarding these devices
- Ensuring 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
- Ensuring that students follow the school's terms on acceptable use (see appendix 2)
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Students:

- responsible for using the school digital technology systems in accordance with the student ICT acceptable user agreement and Cyber safety agreement (see appendix 2)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations and required to sign a plagiarism statement in Year 11
- 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.
- know and understand policies on the taking/use of images and on online-bullying/ harmful sexual behaviours
- 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

Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.

Parents/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
- their children's personal devices in the school (where this is allowed)

Parents/carers are expected to:

- Notify Head of School of any concerns or queries regarding this policy via the email address provided on website
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet as per the RTI Form 4 – parental agreement stating:
    - *I give consent for my son/daughter to access the Internet. I understand that The Jubilee Academy will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the internet facilities.*

Parents can seek further guidance on keeping children safe online safety link hub on the school website

https://www.thejubileeacademy.org.uk/oslinkhub

Visitors and External Agencies:

Visitors and external agencies who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. They will be expected to sign and agree to the terms on acceptable use (appendix 3).

Online Safety Group:

The Online Safety Group (OSG) provides a consultative group that has wide representation from the school community with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives.

The group will also be responsible for regular reporting to the Governing body

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Lead (or other relevant person, as above) with:

- To deliver in accordance with the OSG Terms of Reference

- reviewing and updating the Online Safety policy and associated policies and agreements on a regular basis (at least annually) with stakeholder input and ensuring that Online Safety is integrated with other appropriate school policies and procedures.
- the production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the online safety/ curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs to inform future areas of teaching/learning/training
- consulting stakeholders – including parents/carers and the students about the online safety provision
- Keeping up to date with new developments in online safety.

Professional Standards

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

Policy

Online Safety Policy

The school's Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels via email and Teams

Acceptable use

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- student planners
- staff induction and handbook
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents/carers

- built into education sessions
- school website
- peer support.

Some internet activities e.g. accessing child abuse images or distributing racist material is illegal and 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.

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:

User Actions

User Actions		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
	N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
	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				X	
	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools/academies will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)			X	X		
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping/commerce			X			
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. YouTube			X			

Reporting and responding to incidents of misuse

All online safety incidents whether illegal or non-illegal should be reported via email to the DSL and logged as an incident on CPOMS, additionally the DSL should provide staff with the online safety incident form found in appendix 6 for the reporting member of staff to complete.

The school encourages a safe and secure approach to the management of the incident that might involve illegal or inappropriate activities (see "User Actions" above).

Actions will be taken in accordance with appropriate incident reporting flowcharts in appendix 7

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 flowchart in appendix 8) for responding to online safety illegal in.

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 illegal infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, the Illegal incident will always need to be escalated to the DSL.

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

Once escalated all steps in this procedure should be followed by the DSL:

- Have more than one senior member of staff involved in this process ideally including the DHT Disciple and conduct and/or SBM H&S (ICT). This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated laptop that will not be used by students 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:
    - Interview/counseling by an appropriate member of staff;
    - Informing parents/carers;
    - Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework;
    - Exclusion;
    - Referral to the police.
- **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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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.**

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.

Responding to Learner actions

The school will deal with incidents that involve inappropriate rather than illegal misuse. Any incidents will be 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:

(X – Action always taken, \ - Action may be taken, determined on a case-by-case basis)

	Actions/Sanctions									
Students/Pupils Incidents	Refer to class teacher/tutor	Refer to DSL and SBM H&S (ICT)	Report to DHT Discipline and Conduct	Refer to Head of School	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning/Counselling	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).	\	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X	X	\		X	\	\	X	\
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	\	X	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/academy network by sharing username and passwords	X	X	X	\		X	\	\	X	\
Attempting to access or accessing the school/academy network, using another student's/pupil's account	X	X	X	\		X	\	\	X	\
Attempting to access or accessing the school/academy network, using the account of a member of staff	X	X	X	X	\	X	X	X	X	X

Corrupting or destroying the data of other users	\	X	X	X		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	X
Continued infringements of the above, following previous warnings or sanctions	\	X	X	X		X	X	X	X	X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school	\	X	X	X	\	\	X	X	X	X
Using proxy sites or other means to subvert the school's/academy'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	\
Deliberately accessing or trying to access offensive or pornographic material	X	X	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	X	X	\	\	X	\	X	\

Responding to Staff Actions

All actions marked in this table demonstrate potential actions following an investigation

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a 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	x	x	x
Deliberate actions to breach data protection or network security rules.	x	x	x	x	x	x	x	x
Deliberately accessing or trying to access offensive or pornographic material	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	x	x	x
Using proxy sites or other means to subvert the school's filtering system.	x	x			x	x		x
Unauthorised downloading or uploading of files or file sharing	x	x			x	x		x
Breaching copyright or licensing regulations.	x	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		x
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	x	x		x	x	x	x	x
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	x	x			x	x	x	x
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	x				x	x		
Careless use of personal data, e.g. displaying, holding or	x				x	x		

transferring data in an insecure manner								
Actions which could compromise the staff member’s professional standing	x							
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	x	x				x		
Failing to report incidents whether caused by deliberate or accidental actions	x							
Continued infringements of the above, following previous warnings or sanctions.	x	x	x	x	x	x	x	x

Online Safety Education Programme

The education of the school community in online safety is an essential part of the school’s online safety provision.

Educating Governors about online safety

A named governor for safeguarding and child protection is required to complete training on safe internet use and online safeguarding issues as part of their safeguarding training and invited to participate in school training/information sessions for staff.

Educating staff/volunteers about online safety

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, harmful sexual behaviours and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff briefings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don’t want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training and education will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- recognise current and recent issues and trends of student online activity and habits both in and out of school

- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy will undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Further information about:

- Preventing and addressing Cyber Bullying can be found in appendix 11
- Harmful sexual behaviours inc. sexual harassment and violence and online sexual abuse can be found in appendix 12

Educating students about online safety

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.

All schools must teach:

- Relationships and sex education and health education in secondary schools

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 during PSHRE, assemblies, tutorial/pastoral activities and student voice in the following ways:

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact, conduct and commerce, and know how to report concerns via the school internal systems or appropriate external system e.g. CEOP

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns via the school internal systems or appropriate external system e.g. CEOP

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- How to build 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.
- How to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information and to acknowledge the source of information used and to respect copyright
- To consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable.

When educating students with the use of online capable technologies, **staff** should be aware that:

- Students should be helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technician and Researcher (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Educating parents/carers about online safety

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:

- Letters, newsletters, web site,
- Parents/carers evenings and curriculum events

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL via email at safeguarding@thejubileeacademy.onmicrosoft.com

Concerns or queries about this policy can be raised with the head of school via the email address listed on the school website.

Education – The Wider Community including external agencies

The school will provide opportunities for members of the community and external agencies to gain from the school's/academy's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing online safety expertise/good practice with commissioning schools
- education on the school's culture in relation to Online Safety and the associated policies and agreements

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of ambassadors
- the Online Safety Group has learner representation
- learners contribute to the online safety education programme e.g. peer education, online safety campaigns
- contributing to online safety events with the wider school community e.g. parents' evenings

Technology: infrastructure/ equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school will ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection

Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

Technical Security

The school's technical security including filtering and password policy details how the school will implement technical measures, appropriate policies and procedures and provide education and training in order to ensure that the school's ICT infrastructure is as safe and secure as is reasonably possible.

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

Managing the provisioning privileged IT account

The provisioning privileged IT accounts policy which details how administration roles and responsibilities are properly understood, implemented and used appropriately.

Managing the internet

- Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for student use and will include filtering appropriate to the age of the young people;
- Before being allowed controlled access to internet, all staff must read and sign a copy of the:
  - Safe Working Practice Agreement- Safeguarding Students and Young People (see appendix 4) and
  - Staff ICT Acceptable User Agreement (see appendix 1)
- Staff will ensure students understand and follow the Online Safety Policy and follow the school's terms on acceptable use (see appendix 2)
- Staff will ensure they monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies about these devices
- The school community will report via the school internal systems or appropriate external system if they experience material that they find unsuitable, distasteful, uncomfortable, threatening or harmful;
- To control incoming traffic the school has internet filter installed to ensure computers are not compromised when staff hover on or click on what looks safe.

Managing email

- The school uses Microsoft Outlook email service which has a spam filter to respond to spam
- Before being allowed controlled access to this email service all staff must read and sign a copy of the:
  - Safe Working Practice Agreement- Safeguarding Students and Young People (see appendix 4) and
  - Staff ICT Acceptable User Agreement (see appendix 1)
- Personal e-mail or messaging between staff and students should not take place;
- Where Teams is unavailable or inappropriate, staff should use the respective subject e-mail address if they need to communicate with students about their schoolwork (e.g., study leave, course work, remote working) and always use student's school email address.

- Students and staff may only use approved e-mail accounts on the school system and must inform a member of staff immediately if they receive an offensive e-mail;
- Students must not reveal details of themselves or others in any school e-mail communication or by any social media platforms, such as an address, telephone number and must not arrange meetings with anyone;
- Access in School to external personal e-mail accounts may be blocked;
- Staff should not synchronize personal e-mail accounts with school programs (e.g. Chrome, Outlook);
- Excessive social email use can interfere with learning and will be restricted for staff and blocked for students;
- Incoming email should be monitored, and attachments/links should not be opened unless the author is known to minimise threat to viruses and phishing emails
- Training on induction and Online Safety training provide staff with continuous guidance.
- Email best practice guidance is available to all staff which provides guidance on:
    - Accessing account
    - Avoiding legal issues
    - Safety and encryption
    - What to keep and not to keep
    - Suggested communication format
    - Recalling emails

Managing website content

- The Head of School or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate;
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing;
- The school will ensure that the school ethos is reflected on the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material;
- The point of contact on the school website will be the school address, School email and telephone number. Staff or students' home information will not be published;
- Photographs of students and teachers will not be used without the written consent of the student's parents/carers in line with the GDPR;
- The names of students will not be used on the website where possible and only ever with explicit given consent, particularly in association with any photographs;
- Use of site photographs will be carefully selected so that any students cannot be identified, or their image misused;
- Work will only be used on the website with the permission of the student and their parents/carers;
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained;

Managing Teams (School's Learning Platform)

- All Staff and Students have access to Teams to use for professional and educational purposes;
- Teams is managed centrally through Office 365 and all text conversations are recorded;
- Before being allowed controlled access to Teams all staff must read and sign a copy of the:
    - Safe Working Practice Agreement- Safeguarding Students and Young People (see appendix 4) and
    - Staff ICT Acceptable User Agreement (see appendix 1)

  All students must read and sign a copy of the:
    - Student ICT Acceptable User Agreement (see appendix 2) and
    - Cyber safety agreement (see appendix 2)
- Personal messaging between staff and students should not take place;
- Students' configured policies prevent them from directly messaging each other or messaging staff without staff first messaging them;
- All Teams meetings should be conducted professionally and where webcams are used backgrounds

should be blurred, especially when meeting with external persons;

- Staff should avoid using the recording function when holding meetings;
- In cases where a meeting/training may need to be recorded, the staff member holding the meeting should acquire written consent from all members of the meeting;
- Staff should ensure that the sharing of images and videos does not breach image rights and copyrights. Seek permission from anyone included in personal photographs prior to sharing them;
- Students should avoid sending or sharing images or videos except when the media is a required piece of work;
- Information shared within Teams is for use by the Teams members only and should not be shared outside of the Team without appropriate permissions. No Confidential, Personal or Sensitive information should be shared outside your Teams or the school;
- Students must not reveal details of themselves or others in any communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone;
- All conversations should be kept relevant to the chat or Team;
- Training on induction and Online Safety training provide staff with continuous guidance;
- TJA reserves the right to remove inappropriate MS Teams sites or posts

Managing Information held

- The school conducts regular information audits to gain a clear and common understanding of the range of information assets it holds and those that are critical to business and ensure GDPR compliance.
- The school's information management of records policy offers further guidance on managing information
- Personal data sent over the network will be encrypted or otherwise secured.

Mobile Technologies including BYOD/BYOT

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is for professional and educational purposes. The school's mobile technologies including BYOD and BOYT policy is consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy and acceptable user agreements.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				*Students*			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school/academy	y							y
Use of mobile phones in lessons				y				y
Use of mobile phones in social time		y						y
Taking photos on mobile phones/cameras			y					y
Use of other mobile devices e.g. tablets, gaming devices		y						y
Use of personal email addresses in school/academy, or on school/academy network		y						y
Use of school/academy email for personal emails				y				y
Use of messaging apps		y						y
Use of social media		y						y
Use of blogs		y						y

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, social media, school's Learning Platform 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.

- students will be provided with individual school email addresses for educational use.
- Students will 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.

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 and grooming including online sexual abuse 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. On occasion it may be necessary for the school 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:

The school will educate students about the risks associated with the taking, use, sharing, publication and distribution of images. The risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of students are published on the school website and associated media
  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 the digital/video images.
- Staff, external agencies and volunteers are required attain permission 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/academy 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 associated media, particularly in association with photographs.
- Staff must report any concerns relating to any inappropriate or intrusive photography to the Designated Safeguarding Lead.
- Staff must not use any images that are likely to cause distress, upset or embarrassment.
- Photographs taken by staff on school visits may be used in the curriculum and displayed within the school or at parents' evenings to illustrate the work of the school except in cases where the parent/carer has opted their child out.
- Digital images captured on CCTV are covered in the school's CCTV policy

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

*The DSL may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Refer to Behaviour Policy; and Searching, Screening and Confiscation Policy

Social Media

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school has a social media and networking policy that details the measures the school takes to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff
- 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Social networking and chat rooms for students/parents

- Students will be taught about social media and networking platforms and their safe use;
- Students will not access social networking sites e.g. ‘Instagram’, ’Facebook’ or ‘Twitter’ on site;
- Students will be taught the importance of personal safety when using social networking sites, chat rooms and forums;
- Students will not be allowed to access public or unregulated chat rooms or forums on site;
- Students will only be allowed to use regulated educational chat environments and use will be supervised;
- Newsgroups will be blocked unless an educational need can be demonstrated;
- Students will be advised to use nick names and avatars when using social networking sites off site;
- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil/parent is necessary, the agreement of the Head of School should always be sought first, and language should always be appropriate and professional.

Social Media – official school social media account

Schools are increasingly using social media as a powerful learning tool and means of communication. The school’s professional social media policy provides:

- A chain of approval
- 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

Social Media – personal use

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of 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 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 school permits reasonable and appropriate access to private social media sites
- Staff will not exchange social networking addresses or use social networking sites to communicate with students or parents
- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil/parent is necessary, the agreement of the Head of School should always be sought first, and language should always be appropriate and professional.

Social Media – 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 school

- The school should effectively respond to social media comments made by others according to a defined policy or process

The school’s use of social media for professional purposes will be checked regularly by the Online Safety Group to ensure compliance with the school policies.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website
- Social media
- newsletters
- School information Management System - InTouch

The school website is hosted by E4Education. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

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

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation and as outlined in the school's data protection policy.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up-to-date virus and malware checking software
- data must be securely deleted from the device, in line with school searching and deletion policy once it has been transferred or its use is complete.

Staff must ensure that they

- do not use USB storage devices to carry or transfer any data within or relating to the school
- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

Home and mobile working

Risks Associated with Remote Access

As with all use of technology, there are risks associated with the use of remote access. These risks include but are not limited to:

- Damage or loss of equipment
- Loss of data
- Misuse of data or information – both intentional and unintentional
- Theft of data or information – both intentional and unintentional
- Potential legal action against the school or individuals because of information loss or misuse.
- Potential sanctions against the school or individuals imposed by the Information Commissioner's Office because of information loss or misuse.
- Unauthorised access to confidential information
- Virus or malware infection

Responsibilities of Staff

When using remote access, staff MUST:

- not use public computers for remote access and should only use their own personal equipment or school provided equipment
- only use remote access when in a safe and secure environment
- never leave a device unattended whilst logged into remote access
- always log out of remote access when finished or when taking an extended break.
- act as they would on school grounds: remote access is a professional environment and staff should conduct themselves as such when logged on.
- keep their passwords secure. Passwords must never be given out to someone else (whether employed by TJA or not) and nobody but the person signed in should use remote access
    - Passwords should be memorable enough that they do not need to be written down (as this is prohibited) but also secure enough that nobody could guess it
- never use remote access when logged in as somebody else
- always make sure the device being used to connect to remote access has an up-to-date anti-virus to protect the school system from infection.
- not install programs on the remote desktop, if you need a program installed, please speak to ICT
- not download confidential information from the school systems via remote access to a personal device or to any device other than school issued equipment
- always adhere to the Online safety Policy when using remote access.

Staff will receive training and guidance on best practice when using remote access and be required to sign to agree to abide by the guidelines to use the remote access system responsibly and for work purposes only

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising

- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendices

1. Staff (and Volunteer) Acceptable Use Policy Agreement Template
2. Student Acceptable Use Agreement Template and Cyber Statement
3. External Agency Acceptable Use Agreement Template
4. Safe Working Practice Agreement - Safeguarding Students and Young People
5. Online Safety Training needs - self audit for staff
6. Online Safety Incident report form
7. Online safety Incident Reporting Flowchart
8. Online safety Illegal Incident Reporting Flowchart
9. Online Safety Log
10. Legislation
11. Cyber Bullying
12. Harmful sexual behaviours inc. sexual harassment and violence and online sexual abuse

Supporting Online Safety Policies

13. School Technical Security (including filtering and passwords) Policy
14. Mobile Technologies (inc. BYOD/BYOT) Policy
15. Social Media and Networking Policy
16. Professional Social Media Policy
17. Provisioning Privileged IT accounts Policy
18. Remote Learning Policy

Supporting Safeguarding Policies

19. Safeguarding and Child Protection Training Policy
20. Behaviour Policy
21. Searching, Screening and Confisctaion Policy