Online Safety Policy

2023-2024

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 Key categories of risk

Our approach to online safety is based on addressing the following 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 financial scams.

The school 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

- is published on the school website.

2. Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of St Andrew's VA Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

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

3. Policy development, monitoring and review

This Online Safety Policy has been developed by the Online Safety Group made up of:

- Headteacher/Designated Safeguarding Lead
- Online safety governor
- Oakford
- Admin Officer
- Computing subject lead
- learners (digital leader representatives)

Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	*March 2024*
The implementation of this Online Safety Policy will be monitored by:	*The online safety group*
Monitoring will take place at regular intervals:	*At least annually*
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 regular intervals:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually in Term 4*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- surveys/questionnaires of:
    - learners
    - parents and carers
    - staff

4. Leadership and responsibilities

Responsibilities

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

Headteacher (Designated safeguarding lead)

The Headteacher is responsible for:

- ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding
- ensuring that all staff receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the capability required to keep children safe whilst they are online
- meeting regularly with the online safety committee to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensure that regular filtering and monitoring checks are carried out
- ensuring they and the deputy headteacher (DDSL) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by the Headteacher/DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- Receiving cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- Membership of the school Online Safety Group

Computing Curriculum Lead

The Computing curriculum lead will work with the DSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- class sessions, linked with the school's computing scheme
- online safety assemblies
- PHSE and SRE programmes
- relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week

The computing lead will meet regularly with the online safety committee to discuss current issues.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are 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
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners 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

- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media

IT Provider

The IT Provider (Oakford) is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and action

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- 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

Parents and carers

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

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

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- seeking their permissions concerning digital images, cloud services etc
- newsletters, website and information about national/local online safety campaigns and literature

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

- reinforcing the online safety messages provided to learners in school

Online Safety Group

The Online Safety Group has the following members:

- Headteacher/Designated Safeguarding Lead
- Online safety governor
- Oakford
- Admin Officer
- Computing subject lead
- learners (digital leader representatives)

Members of the Online Safety Group will assist the DSL/OSL 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 education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision, where relevant
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

5. Acceptable use

The acceptable use agreements *(see appendix 1 and 2)* will be communicated/re-enforced through:

- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- education sessions
- school website
- peer support (including digital leaders).

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

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to the Head teacher any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

User actions		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering				X

User actions		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)				X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	
	Promotion of any kind of discrimination			X	
	Using school systems to run a private business			X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school			X	
	Infringing copyright			X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute			X	

	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed in certain circumstances	Allowed for selected staff	Not allowed	Allowed	Allowed in certain circumstances	Allowed with staff permission
Playing games online			X				X	
Online shopping/commerce			X		X			
File sharing		X						X
Social media				X	X			
Messaging/chat	X				X			
Entertainment streaming e.g. Netflix, Disney+		X			X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok		X			X			
Mobile phones may be brought to school		X						X
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school			X		X			
Taking photos on mobile phones/cameras	X				X			
Use of personal e-mail in school, or on school network/wi-fi		X			X			
Use of school e-mail for personal e-mails	X				X			

6. Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead/Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include

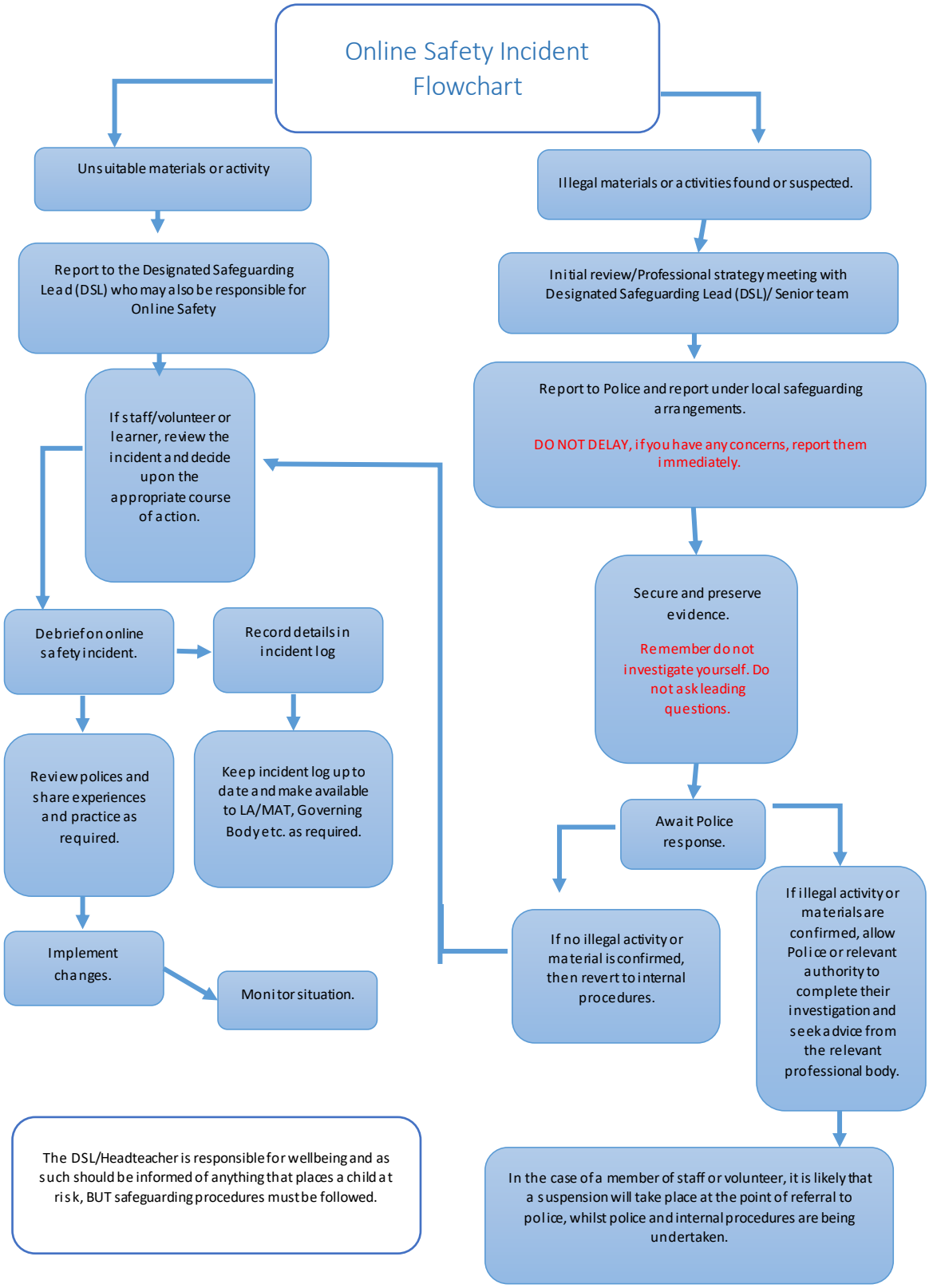
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- 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
    - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- incidents should be logged (cpoms)
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
    - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Illegal materials or activities found or suspected.
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Debrief on online safety incident.
Record details in incident log
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions.
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Await Police response.
Implement changes.
Monitor situation.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department/ Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority/ technical support (Oakford) for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X		X	X		X
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X	X			X		X	X
Corrupting or destroying the data of other users.	X	X	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
Unauthorised downloading or uploading of files or use of file sharing.	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	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X		X	X		Issue advice	
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	X	X
Unauthorised use of digital devices (including taking images)	X	X	X	X		X	X	X	X
Unauthorised use of online services	X	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X	X	X	X	X	X

Responding to Staff Actions

					As a result of previous outcomes, the below could be potential actions		
Incidents	Refer to Head teacher	Refer to local authority/HR	Refer to Police	Refer to local authority/ technical support (Oakford) for advice/action	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on Acceptable use)	X	X	X	X	X	X	X
Deliberate actions to breach data protection or network security rules.	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	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
Using proxy sites or other means to subvert the school's filtering system.	X	X		X	X	X	X
Unauthorised downloading or uploading of files or file sharing	X	X		X	X	X	X
Breaching copyright or licensing regulations.	X	X	X	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		
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	X	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 transferring data in an insecure manner	X			X	X		
Actions which could compromise the staff member's professional standing	X	X			X		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X			X	X	X
Failing to report incidents whether caused by deliberate or accidental actions	X	X			X	X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X	X	X	X

7. Online Safety Education Programme

Online safety is a focus in all areas of the curriculum and staff will reinforce online safety messages across the curriculum. Online safety provision will be provided in the following ways:

- A planned online safety curriculum is taught in a variety of contexts
- Lessons matched to need; are age-related and building on prior learning
- Lessons are context-relevant with agreed objectives leading to clear outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- Incorporating relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.

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 digital leaders*
- *the Online Safety Group has learner representation*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*

Staff/volunteers/governors

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days
- the Designated Safeguarding Lead/Online Safety Lead will provide advice to individuals as required.

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

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

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons.
- letters, newsletters, website, learning platform
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g www.saferinternet.org.uk/; www.childnet.com/parents-and-carers

8. Filtering & Monitoring

The school filtering and monitoring provision is agreed by the DSL, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Filtering

- The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- Younger learners will use child friendly/age-appropriate search engine: Swiggle. This will be the default search engine on laptops, and will be linked for easy use on learner ipads.

- Access to content through non-browser services (e.g. apps) 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.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These include:

- physical monitoring (adult supervision in the classroom)
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- school technical staff regularly monitor and record the activity of users on the school technical systems (during online safety group meetings)

Technical Security

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

- responsibility for technical security resides with SLT who may delegate activities to Oakford.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- the administrator passwords for school systems are kept in a secure place (electronic vault managed by Oakford).
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be reviews and audits of the safety and security of school technical systems
- wireless systems and cabling are securely located and physical access restricted (key stored in office)

- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Oakford and SLT are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/Oakford
- removable media is not permitted unless approved by the SLT/Oakford
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- guest users are provided with appropriate access to school systems based on an identified risk profile.

Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

Personal devices belonging to students will be handed in daily and stored safely in the school office.

The school allows:

	School devices		**Personal devices**		
	School owned for individual use	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	No		
Internet only				Yes	Yes

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- guidance for learners, parents/carers

School staff ensure that:

- No reference should be made in social media to learners, 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.
- they act as positive role models in their use of social media

When official school social media accounts are established, there is:

- a clear process for the administration, moderation, and monitoring of these accounts
- a system for reporting and dealing with abuse and misuse
- an understanding of how incidents may be dealt with under school disciplinary procedures.

Digital and video images

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images

- Learners must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy.
- Learners' 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 learners are taken for use in school or published on the school website/social media.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
- Images will be securely stored.

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

The school website is managed/hosted by Oakford. 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.

Data Protection *(see Appendix 3 - Data Protection Policy)*

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

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (SBM) who has effective understanding of data protection law and is free from any conflict of interest
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which group have responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent).
- has a privacy notice, which lists the lawful basis for processing personal data (including, where relevant, consent). *(See Appendix 3)*

- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

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

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data

- will not transfer any school personal data to personal devices
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

9. 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
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate

10. Appendices

Appendix – A1 – AUA FS/KS1

Student Acceptable Use Policy Agreement

Foundation / KS1

This is how we stay safe when we use technology:

- I will ask a teacher or suitable adult if I want to use the laptops / iPads.
- I will only use activities that a teacher or school adult has told or allowed me to use.
- I will take care of the laptops, iPads and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will talk to my parents/guardian at home about new websites or apps I would like to play on, so they can help me stay safe.
- I know that if I misuse the equipment in anyway, I might not be allowed to use a laptop or iPad in school.

Full name (child): ..... Date: _____

Signed (child): .....

Full name (adult): ..... Date: _____

Signed (parent): .....

As the parent / carer of the above pupil, I understand that the school has discussed the Acceptable Use Agreement with my son / daughter as part of whole school commitment to e-Safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.

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

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Appendix – A2 – AUA KS2

Student Acceptable Use Policy Agreement KS2

This acceptable use agreement is intended:

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

This is how we stay safe when we use technology at school and at home.

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age)
- I will not open emails when I am unsure of the sender or content- instead I will tell an adult.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I understand that the school laptops and iPads should be used for learning purposes and that I will not use them for personal reasons.
- I will not use the school technology for on-line gaming, or video viewing (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will be polite and responsible when I communicate with others, I will not use strong or inappropriate language and I understand that others may have different opinions.
- I will not take or share images of anyone without their permission.
- I will not use my own personal devices in school. They will be handed in to the school office at the start of the school day.
- I will report any damage or problems involving equipment or software straight away, however it may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person who sent the email.
- I will not click on pop ups on websites which seem exciting, as I know that these may take me to inappropriate websites or install viruses etc.
- I will not copy information from school devices onto a personal device nor will I try to alter computer settings.

I understand that I am responsible for my actions, both in and out of school. I should be a responsible and respectful citizen both in real life and online. I understand that if I misuse equipment in any way, I will be subject to disciplinary action.

Full name (child): ..... Date: _____

Signed (child): .....

Full name (adult): ..... Date: _____

Signed (parent): .....

As the parent / carer of the above pupil, I understand that the school has discussed the Acceptable Use Agreement with my son / daughter as part of whole school commitment to e-Safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.

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

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Appendix – A3 – Privacy Notice

Privacy Notice (How we use pupil information)

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as results of national curriculum tests and teacher assessments)
- Relevant medical information (such as that needed to ensure your child's safety and to enable staff to meet your child's medical needs during the school day)
- Special Educational Needs (SEN) information (such as details of any provision that the school has in place for your child, details of SEN assessments, notes of any SEN meetings regarding your child)
- Behavioural information (such as details on exclusions from school, behavioural incidients, as well as achievement information such as Headteacher's Awards) Why we collect and use this information
- Parental permission information (such as permission to use your child's image in photographs or online, and permission for your child to take part in school activities)

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information in accordance with Article 6 and 9 of the GDPR regulations.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for the duration of your child's education. By law, we are required to keep copies of any Child Protection information on our school files until your child's 25th birthday.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- medical professionals (such as the school nursing team, educational and behavioural psychologists)

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact our school office.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/