



Peterhouse School

Online Safety Policy

January 2026

Ruth Smith

POLICY AND PROCEDURE

Online Safety Policy

Policy Number:	Online Safety Policy
Date originally issued:	Nov 16
Date of this review:	January 2026
Date of next review:	January 2027
Director lead for this Policy:	Ruth Smith
Has Consultation included Service User Group?	Yes
Reviewed by:	Ruth Smith
Ratified by Governance Committee on:	13.02.2025

RELATED / RELEVANT POLICIES AND KEY DOCUMENTS

This policy should be read in conjunction with:

Internet Access Policy

Staff AUP agreement

Pupil AUP agreement

Safeguarding Policy

Data Protection Policy

Adult Curriculum Digital Citizenship Policy

Remote Learning Policy

SUMMARY / SCOPE

This Online Safety Policy outlines the commitment of Peterhouse 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, 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).

This policy applies to all members of the school community (including staff, learners, 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).

CONTENTS

1	Scope of the Online Safety Policy	4
1.1	Policy development, monitoring and review	4
1.2	Schedule for development, monitoring and review	4
1.3	Process for monitoring the impact of the Online Safety Policy	5
2	Policy and leadership.....	5
2.1	Responsibilities.....	5
3	Online Safety Group	11
3.1	Professional Standards.....	11
4	Policy.....	12
4.1	Online Safety Policy.....	12
4.2	Acceptable use	12
5	Reporting and responding.....	13

5.1	Responding to Learner Actions.....	17
6	Online Safety Education Programme.....	18
7	Technology.....	22
8	Filtering & Monitoring.....	22
8.1	Filtering.....	23
8.2	Monitoring.....	24
8.3	Technical Security.....	24
8.4	Mobile technologies.....	26
8.5	Social media.....	26
8.6	Digital and video images.....	28
8.7	Online Publishing.....	29
9	Data Protection.....	30
10	Outcomes.....	31
11	Appendix.....	32
11.1	Appendix 2.....	Error! Bookmark not defined.
12	Revision Status.....	37

1 SCOPE OF THE ONLINE SAFETY POLICY

This Online Safety Policy outlines the commitment of Peterhouse 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).

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

Please read this policy alongside:

- AI policy
- Mobile phone policy

1.1 Policy development, monitoring and review

This Online Safety Policy has been developed by the *Online safety group* made up of:

- *Head of School/senior leaders*
- *Designated safeguarding lead (DSL)*
- *Online Safety Lead (OSL)*
- *staff – including teachers/support staff/technical staff*
- *governors*
- *parents and carers*

1.2 Schedule for development, monitoring and review

This Online Safety Policy was approved by the <i>school governing body</i> on:	
The implementation of this Online Safety Policy will be monitored by:	<i>Ruth Smith and the Safeguarding Team</i>
Monitoring will take place at regular intervals:	<i>Termly</i>
The <i>governing body</i> 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:	<i>Termly</i>

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:	Yearly
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding CEOP Police

1.3 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
- internal monitoring data for network activity
- surveys/questionnaires of:
 - learners
 - parents and carers
 - staff

2 POLICY AND LEADERSHIP

2.1 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 individuals¹ and groups within the school.

HEADTEACHER AND SENIOR LEADERS

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

- The Headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff².
- The Headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The Headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

GOVERNORS

The DfE guidance “Keeping Children Safe in Education” states:

“Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare this includes ... online safety”

“Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)”

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

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

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

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

DESIGNATED SAFEGUARDING LEAD (DSL)

Keeping Children Safe in Education states that:

“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder’s job description.”

They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college”

They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online”

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- 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 relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to Head of School/senior leadership team
- be responsible for 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.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

ONLINE SAFETY LEAD

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL).
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments

- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure 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
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - commerce

CURRICULUM LEADS

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. [ProjectEVOLVE](#) .

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

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 have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to [DSL and OSL](#) 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*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- 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 DfE Filtering and Monitoring Standards says:

“Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.”

“Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.”

“The IT service provider should have technical responsibility for:

- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems”*

“The IT service provider should work with the senior leadership team and DSL to:

- *procure systems*
- *identify risk*
- *carry out reviews*
- *carry out checks”*

“We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision.”

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Cyber Security 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 (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from Charity Commission or other relevant body
- 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 DSL or OSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- *monitoring systems are implemented and regularly updated as agreed in school policies*

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

- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

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

3 ONLINE SAFETY GROUP

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group has the following members:

- Designated Safeguarding Lead
- Online Safety Lead
- senior leaders
- teacher and support staff members may attend as appropriate

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
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

3.1 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.

4 POLICY

4.1 Online Safety Policy

The DfE guidance “Keeping Children Safe in Education” states:

“Online safety and the school or college’s approach to it should be reflected in the child protection policy”

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 and through normal communication channels
- *is published on the school website.*

4.2 Acceptable use

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

Acceptable use agreements

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

- learner handbook
- 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.

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.** *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- **staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community**
- **users should immediately report to a 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.**
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*

5 REPORTING AND RESPONDING

The 2021 Ofsted “Review of Sexual Abuse in Schools and Colleges” highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

“School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse”*

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 ([see flowchart and user actions chart in the appendix](#)), 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 Head of School, unless the concern involves the Head of School, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- 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 as relevant
 - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on CPOMS by the end of the day.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - *the 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, school social media, website*
 - *governors, through regular safeguarding updates*
 - *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested “working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour”*

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



SCHOOL ACTIONS

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

5.1 Responding to Learner Actions

Students

Actions

Incidents:	Refer to Online Safety Coordinator	Refer to Head teacher	Refer to Police	Device to stay at home or to be given to class teacher each morning for one week.	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of internet access rights for one day.	Removal of internet access rights for one week	Further Actions
Deliberately accessing or trying to access material that could be considered illegal.	X	X	X		X				X
Unauthorised use of non-educational sites during lessons	X					X	X	X	
Unauthorised use of mobile phone / digital camera / other mobile device	X			X		X	X	X	X
Unauthorised 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 Peterhouse School network by sharing username and passwords	X	X						X	X
Attempting to access or accessing the school network, staff account, the school pod or using another student's account.	X	X				X		X	X
Corrupting or deleting the data of other users	X	X				X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X						X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X					X	X
Using proxy sites or other means to subvert the filtering system	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
Destruction of electronic equipment.	X	X					X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X						X

6 ONLINE SAFETY EDUCATION PROGRAMME

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."

Keeping Children Safe in Education states:

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum ..."

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways (statements may need to be adapted, depending on school structure and the age of the learners).

- A **planned online safety curriculum** for all year groups matched against a nationally agreed framework e.g. **Project Evolve** and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- 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

- it incorporates/makes use of 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.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the [CyberChoices](#) site.*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners 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 learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and 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 should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

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.*
- *the pupil voice group*
- *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*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

STAFF/VOLUNTEERS

The DfE guidance "Keeping Children Safe in Education" states:

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

*"Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."*

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. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff 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. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- *the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

GOVERNORS

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

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

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

FAMILIES

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 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*
- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform,*
- *high profile events / campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).*
- *Sharing good practice with other schools in clusters and or the local authority/MAT*

ADULTS AND AGENCIES

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

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- providing online safety information via their website and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (consider supporting these groups with an online safety review using 360 Groups or 360 Early Years).

7 TECHNOLOGY

The Autism Initiatives IT Support Team 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 should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

8 FILTERING & MONITORING

The DfE guidance (for England) on filtering and monitoring in “Keeping Children Safe in Education” states:

“It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the ... risks from the school’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure 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 appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards...”

The school filtering and monitoring provision is agreed by senior leaders, 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

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

The filtering and monitoring provision is reviewed annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

· Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in

working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering.

8.1 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](#). The school uses Smoothwall and Impero for filtering and monitoring. This includes all school devices which are used offsite as well.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- *the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- ~~younger learners will use child friendly/age appropriate search engines e.g. [SWGfL Swiggle](#)~~
- *the school has a mobile phone policy and 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.*

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content site](#).

8.2 Monitoring

The school has monitoring systems in place (Impero and Smoothwall) 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 may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

8.3 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 the Autism Initiatives Head of IT who may delegate activities to identified roles.
- 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
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- 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.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- 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,
- The AI Head of IT is 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.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- 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/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile.

8.4 Mobile technologies

The DfE guidance “Keeping Children Safe in Education” states:

“The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.”

Mobile technology devices are school owned/provided and might include smartphone, tablet, wearable devices, 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 cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

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

Please also see mobile phone policy

8.5 Social media

Expectations for teachers’ professional conduct are set out in the [DfE Teachers Standards](#) but all adults working with children and young people must understand that the nature and responsibilities of their work, place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, 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 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 without explicit informed consent.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should 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 should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

PERSONAL USE

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, 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

MONITORING OF PUBLIC SOCIAL MEDIA

- As part of active social media engagement, the school may 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.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

8.6 Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate 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 is 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 DfE and Autism Initiatives guidance concerning the sharing, storage, distribution and publication of those images*
- *care should be taken when sharing digital/video images that learners are appropriately dressed*
- *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 in line with the school retention policy*
- *learners' work can only be published with the permission of the learner and parents/carers.*

8.7 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 Concept4. 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 school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

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

9 DATA PROTECTION

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

The school:

- Follows the Autism Initiatives Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The 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, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data

- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- provides data protection training for all staff at induction and appropriate refresher training thereafter. 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 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 (below) 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.

10 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

Flexible Education

Some Flex Education pupils access learning from their home environment. If a pupil is accessing a school device at home it is monitored by Smoothwall with the school policies in place even if it is connected to their own internet. During sessions if technology is being used to support learning as a planned activity then school devices are used.

When pupils are on their own devices in their own homes during the school day it is parental responsibility to monitor the young person's internet activity and if parents have any concerns they are aware they need to report it to the school.

If staff have concerns regarding online safety in the home environment they follow the online safety policy and report it via CPOMS.

11 APPENDIX

Staff and Volunteer Acceptable Use Policy Agreement

Please see "Acceptable Use of I.T. Resources Policy (including Acceptable Use of Internet, Email & Social Media)" for Autism initiatives

Parents/ Carers Acceptable Use Policy 2025

I know that my child will receive digital (online) safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

I am aware that any internet and computer use using school equipment is monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with Department for Education requirements, data protection and human rights legislation.

I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that my child must hand their phone or technology in when they come into school.

I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted. If the school believes that my child has committed a criminal offence then the Police will be contacted

I know that I can speak to the school online safety Coordinator, my child's teacher or the Head Teacher if I have any concerns about digital safety.

I can visit the school website <https://www.peterhouseschool.com/online-safety/> for more information about the school's approach to digital safety as well as to access useful links to support both myself and my child in keeping safe online at home

I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online

I will support the school and my child by sharing responsibility and role modelling safe and positive online behaviour for my child and by discussing online safety with them when they access technology at home.

I, together with my child, will support the school's approach to digital safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

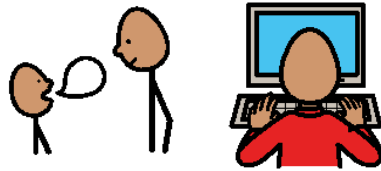
Social networking and media sites: I understand that the school has a clear policy on The use of social networking and media sites and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I understand that if I have any concerns or complaints, I will contact the school directly to ensure that these can be addressed promptly and effectively. I understand that social media is not an appropriate forum for addressing concerns and complaints.

Peterhouse Acceptable Usage Policy – Semi formal

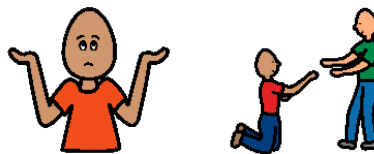
I will ask an adult when I want to go online



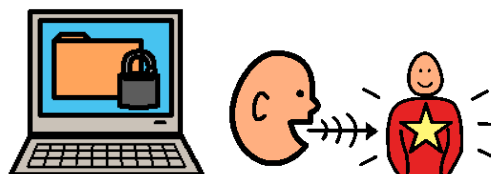
I will try to listen and follow staff instructions when I'm online



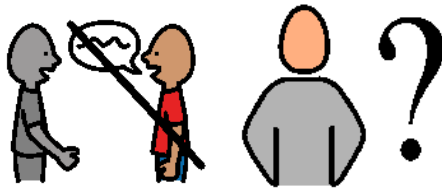
I will ask staff for help if I'm unsure



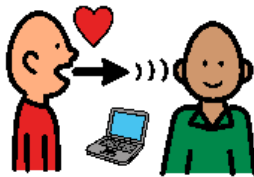
I will only share personal information, like passwords, with people I know and trust



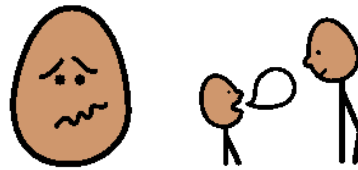
I will never speak to or meet up with people I do not know



I will always be kind when I'm online



If I feel worried or unsure about something online, I will speak to an adult



Peterhouse Acceptable User Policy – 2025

- I use my school technology for school work unless I have permission otherwise
- I will keep my passwords safe
- I only send messages online which are polite and friendly
- I only talk with and open messages from people I know and I only click on links if I know they are safe
- I keep my personal information safe and private online
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult
- I will only post pictures or videos on the Internet if they are appropriate and if I have permission from the person.
- I will only change the settings on the technology if a teacher/technician has allowed me to.
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I will not access or change other people's files or information
- I know that my use of school computers and internet access will be monitored
- If I am aware of anyone being unsafe with technology then I will report it to a teacher
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away.
- I have read and talked about these rules with my parents/carers
- I will not use my mobile phone while in School.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- I will not use personal devices such as; USB pens, camera's or video's in school for any reason.
- I know that bullying in any form is not tolerated.

I will take care of my device whist at home or in school by:

- Treating the device with care at all times and transport safely.
- Keeping the device in a secure place when not in use
- Not leaving the device in a car or on show at home
- Not eating or drinking around the device
- Not lending the device to friends
- Not lending the device to siblings
- Not leaving the equipment unsupervised in unsecured areas

Student Name:

Student Signature:

12 REVISION STATUS

This Review Date	Details of Changes	Sections Changed	Author	Date of next review
20/2/18	Staff AUP Student AUP	Section 11	CW	Feb 19
Jan 19	E-Safety Council Removed	Section 3	CW	Nov 19
March 19	Use of encrypted pen drives no longer permitted.	Appendix 1	CW	Nov 19
November 19	Work emails personal devices.	Appendix 1	CW	November 20
November 20	Remote Learning Policy added page 1	Relevant Policy's and Key documents	CW	November 21
November 20	Appropriate Use Agreement updated to include home learning.	Appendix 2	CW	November 21
September 22	Updates from 360 online	Throughout policy	RS	October 23
October 23	Updates throughout including adding information regarding KCSIE	Throughout policy	RS/CB	September 24
Endorsed by the Education Services Governance Committee – 19.04.24				
January 2025	Updated Acceptable User Policy for parents, staff and pupils	Appendix 2	RS and CB	January 2026
Endorsed by the Education Services Governance Committee on the 13.02.2025				
January 2026	Updated referring to other policies	Mobile Phone	RS	January 2027
To be endorsed by Peterhouse Governance Committee – 12.02.2026				

