Paxcroft Primary School

Online Safety Policy

Reviewed: September 2024

Next date or review: September 2025

ON LINE SAFETY

This policy should be read and understood in conjunction with the following documents:

- Acceptable Use Agreements
- Behaviour Policy
- Bulling Policy
- Child Protection Policy
- Data Protection and Secure Data Handling Policy
- Remote Learning Policy
- Social Networking Policy (WSCB)
- Staff Code of Conduct
- Guidance for Safer Working Practice for Adults working with Children and Young People (February 2022)
- Keeping Children Safe in Education (DfE)
- Screening, Searching and Confiscation advice for schools (DfE 09/22)
- Education for a Connected World framework (UK Council for Internet Safety 2020 Edition)
- Teaching online safety in schools (DfE Published January 2023)
- Teachers' Professional Standards (DfE Updated December 2021)
- SWGfL Project Evolve – online safety curriculum programme and resources
- UK Council for Internet Safety (UKCIS) – Online safety in schools and colleges: questions from the governing board (Pub 2/11/16; last updated 6/10/22)
- Meeting digital and technology standards in schools and colleges (DfE published 03/22, updated 01/24)
- Mobile phones in schools: Guidance for schools on prohibiting the use of mobile phones throughout the school day (DfE Published 02/04)
- Toolkit for schools – communicating your policy for prohibiting the use of mobile phones in schools with parents (DfE Published 02/24)

APPENDICES:	
1	**Staff and Volunteer Acceptable Use Agreement**
2	**Parent Acceptable Use Agreement**
3	**Pupil Acceptable Use Agreement (Younger Children)**
4	**Pupil Acceptable Use Agreement (KS2)**
5	**Online Safety Incident Flow chart**
6	**Procedures to handle incidents of misuse, including responding to illegal incidences (flow chart)**
7	**Technical security (including filtering, monitoring and passwords)**
8	**Form to request temporary removal of filtering**

CONTENTS:

1. Scope of the policy
2. Aims of the policy
3. Policy development, monitoring and review
4. Acceptable use agreements
5. Roles and responsibilities:
    a. Head teacher and senior leaders
    b. School Governors
    c. Online Safety Lead (OSL)
    d. Designated Safeguarding Lead (DSL)
    e. Curriculum leads
    f. Teaching staff, support staff and volunteers
    g. Network manager & technical staff
    h. Pupils
    i. Parents
    j. Community users
6. Online safety group
7. Reporting and responding
8. Education and training
    a. Education of pupils
    b. Contribution of pupils
    c. Staff and volunteers
    d. Governors
    e. Parents
    f. Adults and agencies
9. Technology
    Filtering and monitoring
    a. Filtering
    b. Monitoring
    c. Technical security
    d. Mobile technologies (including BYOD/BYOT)
    e. Digital and video images
    f. Online publishing
    g. Date protection
10. Social media
    a. School use
    b. Personal use
    c. Monitoring of social media
    d. Cyberbullying (including sexting)
11. Outcomes
12. Handling of complaints

1. Scope of the policy

- This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents[1], visitors and community users) who have access to and are users of school's 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.
- The Education and Inspections Act 2006 empowers head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.
- The 2011 Education Act and The Schools (Specification and Disposal of Articles) Regulations 2012 increased these powers with regard to the searching for and of electronic devices and the deletion of data as did well as the guidance from the DfE entitled Screening, Searching and Confiscation at schools (DfE 09/22)
- The school will deal with such incidents within this policy and associated policies as referenced above and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

2. Aims of this policy:

The Online School 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 and flowcharts
- is made available to staff at induction and through normal communication channels
- is published on the school website.

3. Policy development, monitoring and review

This Policy has been developed by a working group/committee made up of:

- head teacher and senior leaders
- Designated Safeguarding Lead (DSL)
- Online Safety Lead (OSL) (if not the DSL)
- staff – including teachers, support staff and technical staff
- governors

---

[1] **parents**' refers to birth parents and other adults who are in a parenting role, for example step-parents foster carers and adoptive parents

- parents

Schedule for the development, monitoring and review of this policy

This online safety policy was approved by the school governing body on:	*Insert date*
The implementation of this online safety policy will be monitored by the:	*DDSL – Mr A George*
Monitoring will take place at regular intervals:	*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 developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2025*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA Safeguarding Officer, LADO, Police, as appropriate*

The school will monitor the impact of the policy using:

- logs of reported incidents
- filtering and monitoring logs
- internal monitoring data for network activity
  -

4. Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the schools. The acceptable use agreements are documents that outline the school's expectations on the responsible use of technology by its user. We require all users to read and understand the contents and importance of these agreements and ask parents to ensure that their children also clearly understand their responsibilities. They will be communicated and reinforced through:

- learner handbook
- staff induction and handbook
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents
- built into education sessions
- school website
- peer support

5. Roles and 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. Whilst this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

- Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report any such incident to a senior manager. This is as relevant in the online world as it is in the classroom; staff engaging with pupils and/or parents online have a responsibility to model safe practice at all times.
- In addition to the roles and responsibilities outlined below, and to support the implementation of this policy, the school has compiled 'Acceptable Use Agreements' (AUAs), which provide clear guidance in relevant areas such as conduct, access to and use of the school system, removable media, downloading files, sharing information, social networks and devices (both school and personal equipment within and outside school).
- Separate agreements have been written for:
  - staff and volunteers
  - governors
  - pupils
  - parents

  who are all expected to read and sign them to acknowledge their responsibilities in this area.
- All key stakeholders, including the school IT service provider, have a responsibility for safeguarding young people from computer misuse and are aware of the Cyber Choices programme.[2]

a. Head teacher and senior leaders:

- The head teacher 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 DSL as defined in 'Keeping Children Safe in Education'.
- The head teacher and (at least) another member of the senior management team (SMT) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (Appendix 6 – 'Procedures to handle incidents of misuse, including responding to illegal incidences (flow chart)' and relevant Local Authority disciplinary procedures.
- The head teacher and SMT are responsible for ensuring that the DSL, OSL, IT providers/technical staff, and other relevant staff, carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and to train other colleagues, as relevant.
- The head teacher and SMT 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 head teacher and SMT will receive regular monitoring reports from the OSL**.**
- The head teacher and SMT will work with the responsible Governor, the DSL and IT service providers in all aspects of filtering and monitoring

b. School Governors

- Governing bodies should ensure that online safety is a running and interrelated theme whilst devising and implementing their whole school approach 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.
- A member of the Governing Body has taken on the role of the Online Safety Governor and the governor with that responsibility is Ms Alexandra Doogue.

---

[2] The Cyber Choices programme is led by the National Crime Agency (NCA) and managed locally by Regional Crime Units

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the question posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".
- This review will be carried out by the Online Safety Governor, Safeguarding Governor and school DSL receive regular information about online safety incidents and monitoring reports. Updates and information about online safety incidents and monitoring reports from the OSL.
- The role of the Online Safety Governor will include:
    - regular meetings with the DSL/OSL
    - regularly receiving (collated and anonymised) reports of online safety incidents
    - checking that provision outlined in this 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 members of the SMT, the DSL and the IT service provider and involve the responsible governor) in line with the DfE Filtering and Monitory Standards.
    - reporting to relevant Governors/Committee/meeting The governing body will support the school in encouraging parents and the wider community to become engaged in online safety activities.

c. Designated Safeguarding Lead (DSL)

The DSL will :

- hold the lead responsibility for online safety within the 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 internet knowledge and up to date capacity required to keep children safe whilst they are online, including a good understanding of the risks to young people of cybercrime and computer misuse
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that the annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body/subcommittee meetings
- report regularly to the head teacher/SMT
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensure that all incidents are recorded
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

c. Online Safety Lead (OSL)

The OSL will be a member of the SMT and their responsibilities are to:

- lead the Online Safety Group
- work closely on a day to day basis with the DSL where these roles are not combined
- 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 reviewing the school's online safety policy, procedures and documents
- promote an awareness and commitment to online safety education/awareness, raising concerns across the school and beyond
- 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 (i.e. misuse – see Appendix 6)
- provide (or identify sources of) training and advice for staff, governors, parents and pupils

-
- liaise with the Local Authority (LA) and other external agencies as relevant
- liaise with the school's technical support and external providers as relevant
- receive regularly updated training to allow them to understand how digital technologies are used and are developing, particularly by pupils, with regard to the areas defined in KCSiE:
    - **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.

Curriculum leads

- Curriculum Leads will work with the DSL/OSL to develop a planned an coordinated online safety programme (e.g. ProjectEVOLVE), with reference to the DfE guidance: 'Teaching online safety in schools' (January 2023).
- This will be provided through:
    - a discrete programme
    - RSE programmes
    - a mapped cross-curricular programme
    - assemblies and pastoral programmes
    - through relevant initiatives and opportunities e.g. Safer Internet Day and Anti-Bullying Week

d. Teaching staff, support staff and volunteers

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, including the potential for risks of computer misuse
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable AUA
- they immediately report any suspected misuse or problem to **the DSL** or investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents should be on a professional level, professional in tone and content and only carried out using official school systems, emails and technologies that are officially sanctioned by the school
- online safety issues are embedded in all aspects of the curriculum and other activities
- 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 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- they have 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.

g. IT Provider

The DfE 'Filtering and Monitoring Standards' state that: "Senior leaders should work closely with governors or proprietors, the DSL and IT service providers in all aspects of filtering and monitoring. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective."

- 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 closely with the SMT and DSL to:
    - procure systems
    - identify risks
    - carry out reviews
    - carry out checks
- The IT Provider is responsible for ensuring that:
    - they are aware of and follow the school's Online Safety Policy and Technical Security Procedures 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 and colleges' and guidance from local authority/MAT 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 the DSL for investigation and action
    - the filtering procedures are applied and updated on a regular basis and their implementation is not the sole responsibility of any single person
    - monitoring software/systems are implemented and regularly updated as agreed in school policies

h. Pupils

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

i. Parents

- Parents are responsible for using the school's digital technology systems in accordance with the 'Parents' AUA' which they are required to read and sign when their child joins school.
- Parents play a crucial role in ensuring that their children understand the need to use internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through:
    - publishing the school Online Safety Policy on the website
    - providing them with a copy of the learners' AUA
    - publishing information about appropriate use of social media relating to posts concerning the school
    - seeking their permissions concerning digital images, cloud service etc
    - parents' evenings, newsletters, the school's website, social media and information about national and local online safety campaigns and literature
- Parents will be encouraged to support the school in:
    - reinforcing the online safety messages provided to pupils in school
    - following guidance on the appropriate use of digital and video images taken at school events and in their access to parents sections on the school's website, learning platforms and online pupil records
    - following the school's guidance on the use of their children's personal devices in the school (where this is allowed)

6. Reporting and Responding

- It is more than 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 the members of the school community are aware that incidents have been dealt with. Such incidents of misuse will be dealt with through the school's normal behaviour and disciplinary procedures.
- There may however be occasions when the school has to respond to reports of illegal misuse and, whilst the school will take all reasonable precautions to ensure online safety for all school users, we recognise that incidents may occur inside and outside of the school (with impact on the school) which will need intervention.
- All staff will be made aware of the flow charts which make up Appendices 5 and 6: "Online Safety Incident" (Appendix 5) and "Responding to Incidents of misuse" (Appendix 6).
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously, dealt with effectively and that there are support strategies in place (e.g. peer support) for those reporting or affected by an online safety incident.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues (e.g. local authority, Professional Online Safety Helpline, Reporting Harmful Content, CEOP).
- The school will ensure that:
    - there are clear reporting routes which are understood and followed by all member of the school community, which are consistent with the school's safeguarding procedures (including the management of allegations) as well as the school's policies on whistleblowing and complaints
    - all members of the school community are 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
    - those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions as relevant
- the DSL and OSL, together with other responsible staff, will 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 Appendix 6) 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 exploitation grooming
    - extreme pornography
    - sale of illegal materials/substances
    - cyber or hacking offences under the Computer Misuse Act
    - copyright theft or piracy
- Incidents should be logged using the school's system.
- 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 effective the report was dealt with
    - staff, through regular briefings
    - learners, through assemblies/lesson
    - parents through regular safeguarding updates
    - local authority and other external agencies as relevant

7. EDUCATION AND TRAINING

a. Education of pupils

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety, digital competence and digital literacy is therefore an essential part of the school's online safety provision and should be effectively threaded through the appropriate pillars in other curriculum areas,e.g. PHSE, RHE/SRHE, Literacy etc
- Pupils should be helped to understand the need for the 'Pupil 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 and with reference to the Computer Misuse Act.
- The school curriculum is designed and written with reference to the key documents listed below, ensuring relevance, breadth and progression in the content to reflect the different and escalating risks that pupils face and covering the principles of online safety:
    - Teaching online safety in schools (DfE Published June 2019/updated January 2023)
    - Education for a Connected World framework (2020 Edition published by the UK Council for Internet Safety)
    - SWGfL Project Evolve – online safety curriculum programme and resources
    - Computing Curriculum (DfE 2013)
- To ensure the quality of learning and outcomes, the online safety curriculum should be broad, up-to-date, provide opportunities for creative activities and context-relevant with agreed objectives, which are age-related, built on prior learning and lead to clear and evidenced outcomes.
- Given the rapid changes in this area the school's provision should be regularly revisited.
- Learners needs and progress are address through effective planning and assessment.

- Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience. This includes:
    - how to use technology safely, responsibly, respectfully and securely
    - where to go for help and support when the have concerns about content or contact on the internet or other online technologies.
- The programme will be accessible to learners of 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.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of the information.
- As part of the relationship and health education curriculum, pupils are taught about online safety and harms. This includes being taught:
    - what positive, healthy and respectful online relationships look like
    - the effects of online actions on others
    - how to recognise and display respectful behaviours on line
- Key on line safety messages should also be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- In lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would require them to access sites normally blocked by the school's filtering system. In such cases, staff can request that filters can be temporarily removed from those sites for the period of study. Any request to do so, should be auditable, with clear reasons for the need and in line with the school's procedures.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

b. Contribution of pupils

- The school acknowledges, learns from, and uses the skills and knowledge of pupils 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 pupil feedback and opinions
    - by the appointment of digital leaders/anti-bullying ambassadors/peer mentors
    - by pupil representation on the Online Safety Group
    - through pupils representation on the online safety education programme, e.g. peer education, digital leaders, leading lessons for younger learners and online safety campaigns
    - by pupils contributing to the writing and updating of the pupil AUA
    - pupils contributing to online safety events with the wider school community, e.g. parents' evenings family learning programmes etc.

c. Staff and volunteers

- All staff will receive online safety training and understand their responsibilities, as outlined in this policy.

- The DSL/OSL will receive regular updates through attendance at external training events (e.g. from the South West Grid for Learning (SWGfL)/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- The OSL will provide advice, guidance and training to individuals as required.
- Training to all staff will be offered as follows:
  - a planned programme of formal online safety and data protection training will be made available to all staff, which will be regularly updated and reinforced
  - an audit of the online safety training needs of all staff will be carried out regularly and individual requirements identified through their performance management
  - the training will be an integral part of the school's annual safeguarding and data protection training for all staff
  - training will include explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
  - all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements/Code of Conduct
- All staff are made aware of the safeguarding issues of computer misuse and are familiar with the NCA Hacking it Legal Leaflet, which explains cyber choices and the Computer Misuse Act 1990, together with a list of recommended resources for teachers.
- Where staff are unsure of their responsibilities or recognise a lack of understanding and therefore a need for further training, they must raise this with their line manager..
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings and/or INSET days as required.

d. Governors

- Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology and online safety, health and safety and safeguarding. This may be offered in a number of ways:
  - attendance at training provided by the LA/MAT, National Governors Association or other relevant organisation (e.g. SWGfL)
  - participation in school training and information sessions for staff or parents, which may include attendance at assemblies and 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 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 reviews.

e. Parents

- Many parents 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 and regulation of the children's online behaviours. They may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
- The school will therefore seek to provide information and awareness to parents through:
  - regular communication, awareness raising and engagement on online safety issues, curriculum activities and reporting routes
  - letters, newsletters, the school's web site and learning platform
  - parents' information sessions through awareness workshops and parents' evenings etc, with the involvement of pupils where appropriate
  - high profile events and campaigns e.g. Safer Internet Day

  - reference to the relevant web sites and publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

f. 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 the use of digital technologies and online safety
- providing online safety information via the school's 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.

8. TECHNOLOGY

The school is responsible for ensuring that its infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

Filtering and Monitoring

- The school's filtering and monitoring provision is agreed by senior leaders, governors and the IT service provider and are 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.
- Checks on the filtering and monitoring system are acaaried out by the IT service provider with the involvement of a senior leader, the DSL and a governor, in particular when a safeguarding risk is identified, there is a change in working practice (e.g. remote access of BYOD, or new technology is introduced.

a. Filtering:

- The school manages access to content across its systems for all users and on all devices using the school's internet provision.. he filtering provided meets the standards defined in the the 'DfE Filtering standards for schools and colleges' and the guidance provided in the UK Safer Internet Centre 'Appropriate filtering'.
- 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 requests for filtering changes (see Appendix 8 for more details).
- Filtering logs are regularly reviewed and alert the DSLl to breaches of the filtering policy, which are then acted upon.
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site .

b. Monitoring

- The school has monitoring systems in place to protect the school, systems and users:
    - the school monitors all network use across all its devices and services
    - an appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored and there is a staff lead responsible for managing the monitoring strategy and processes
    - there are effective protocols in place to report abuse/misuse and there is a clear process for prioritising response to alerts that require rapid safeguarding intervention
    - management of serious safeguarding alerts is consistent with safeguarding policy and practice
    - technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.
- 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 strategy informed by the school's risk assessment including:
    - 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 school monitoring lead(s)*

c. **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 SMT 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 SMT/Online Safety Group
- Password policy and procedures are implemented, (consistent with guidance from the National Cyber Security Centre.
- 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. (See Appendix 7 for further details of the school's 'Technical Security' procedures.)I
- 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 School Business Manager 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 SMT/IT service provider.
- Removable media is not permitted unless approved by the SMT/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.

d. Mobile technologies (including BYOD/BYOT[3])

- Mobile technology devices may be school owned/provided or personally owned 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 the school's learning platform and other cloud based services such as email and data storage.
- The school's acceptable use agreements for staff and volunteers, pupils and parents give clear guidance regarding the use of mobile technologies and these are attached as appendices to this policy.
- The school allows:

	School Devices			Personal Devices		
	School owned for individual use	**School owned for multiple users**	**Authorised device[4]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes* given to member of staff*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*Discretionary*
Internet only				*No*	*Yes*	*Discretionary*
No network access				*Yes*	*No*	*Discretionary*

---

[3] BYOD: bring your own device, BYOT: bring your own technology

[4] 'Authorised device': a device purchased by the pupil/family through a school organised scheme that is given full access to the networks as if it were owned by the school.

- All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational, irrespective of whether the device is school owned or personally owned.
- Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education and is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding and Child Protection Policy, The Behaviour Policy and Bullying Policy, the Staff Code of Conduct, Acceptable use agreements and policies around theft or malicious damage
- Pupils are permitted to bring their own mobile devices into school, including mobile phones and wearable devices, but they must be handed in to their class teacher at the start of the day and returned at the end of the day.

e. Digital and video images:

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

- The 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.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Any images of pupils should only be taken on a school device. The personal device of staff/volunteers must not be used, except in an emergency, when such use must immediately be reported to a member of staff.
- Staff/volunteers must be aware of those learners whose images must not be taken/published and any images of pupils should
- In accordance with guidance from the Information Commissioner's Office (ICO), parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images. This is clearly laid out in the acceptable use agreement for parents. However, there may be occasions where the school requests that parents do not take pictures or videos, but this will only be done if felt absolutely necessary and the school requests that parents are supportive and comply with such requests.
- Staff and volunteers are allowed to take digital /video images to support educational aims, but must follow the school policies concerning the sharing, distribution and publication of those images.
- As required by the Data Protection Act, written permission from parents will be obtained before photographs of pupils are taken for use in school and/or published on the school website/social media. Parents will be informed of the purposes for the use of the images, how they will be stored and for how long, in line the Data Protection and Secure Data Handling .
- Photographs published on the school website, or elsewhere, that include pupils will be carefully selected and will comply with good practice guidance on the use of such images.

- Pupils full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Care will be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupil's work can only be published with the permission of the pupil and parents.

f. <u>Online publishing</u>

- The school communicates with parents and the wider community and promotes the school through:
  - the school's public facing website
  - social media
  - online newsletters
- The school website is managed by Juniper Websites.
- The school ensures that the 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, thus ensuring that there is least risk to members of the school community, through such publications.
- The school's public online publishing provides information about online safety (e.g. the school's Online Safety Policy and Acceptable Use Agreements; curating latest advice and guidance and creating an online safety page on the school website.

g. <u>Data protection</u>

- The school has a comprehensive 'Data Protection and Secure Data Handling Policy' written with reference to current legislation and guidance as issued by the Information Commissioner's Office, which clearly details the school's responsibilities and its staff.
- The school has appointed an appropriate Data Protection Officer who has an effective understanding of data protection law and is free from any conflict of interest.

10. <u>Social media</u>

a. School use:

- 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, 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 and parents
- School staff should ensure that:
  - no reference should be made in social media to learners, parents 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 (acceptable use agreements)

  - systems for reporting and dealing with abuse and misuse
  - understanding of how incidents may be dealt with under school disciplinary procedures.

b. 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
- *the school permits reasonable and appropriate access to personal social media sites by staff during school hours*

c. Monitoring of social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- When parents 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 should be informed of the school complaints procedure.

d. Cyberbullying[5] (including 'sexting'[6])

- Cyberbullying (including 'sexting')can be defined as "the use of technologies by an individual or group of people to deliberately and repeatedly upset someone else"[i]
- For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.
- Cyberbullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's Behaviour, Anti-Bullying and Safeguarding and Child Protection policies, which include:
  - clear procedures set out to investigate incidents or allegations of cyber bullying
  - clear procedures in place to support anyone in the school community affected by cyber bullying
- All incidents of cyberbullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.
- Pupils, staff and parents will be required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.
- Further guidance and advice regarding 'sexting' can also be found through the following links:
  - UKCIS 'Advice for schools: Responding to and managing sexting incidents')
  - DfE December 2020 - Sharing nudes and semi-nudes: how to respond to an incident (overview)

11. Outcomes

---

[5] Childnet.com: 'Understanding cyberbullying'

[6] Sexual violence and sexual harassment between children in schools and colleges (DfE 09/21)

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, pupils and parents; 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 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.

12. Handling of complaints

- Parents and pupils will need to work in partnership with the school to resolve issues.
- Where complaints do not involve acts which are clearly illegal (e.g. accessing child abuse images;distributing racist material; computer misuse and/or cybercrime) they should be dealt with through the school's normal complaints procedures as outlined in the school's Complaints Policy.
- Complaints regarding Illegal activity would be dealt with in line with the school's safeguarding and disciplinary procedures and where required, would involve contact with the police and could lead to criminal prosecution, as could clear cases of cyberbullying.
- As detailed above, there are clear procedures in place to deal with concerns around cyberbullying and such incidences should be brought to the attention of the school as early as possible.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Any complaint about the Head Teacher/Principal should be referred to the Chair of Governors.
- Where any member of the school community has breached the terms of their respective 'Acceptable Use Agreement', the school reserves the right to restrict their access to the school's internet.