Highlands
School & Sixth Form

Dare to
flourish

Online Safety Policy

APPROVED

Date of last review	September 2025
Next review due	September 2027
Governor Committee	School Standards & Performance

Contents

Section 1: Introduction

Scope of the 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”

This online safety policy outlines the commitment of Highlands school to safeguard members of our school community online in accordance with statutory guidance and best practice. This policy applies to all members of the school community (including staff, students, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's digital technology systems, both in and out of the school.

The school's Online safety policy is based on a whole-school approach and addresses the four categories of online risk, known as the 4 Cs:

- Content: Exposure to illegal, inappropriate, or harmful material. In line with KCSIE 2025, this explicitly includes safeguarding against exposure to misinformation, disinformation (including 'fake news'), and conspiracy theories.
- Contact: Harmful interactions with others, such as online grooming, exploitation, or harassment.
- Conduct: Inappropriate online behaviour, whether deliberate or accidental, such as bullying, viewing illegal content, or sharing private data.
- Commerce: Risks related to online financial transactions, gambling, and fraud.

What is online safety?

The school’s online safety policy reflects the importance it places on the safe use of information systems and electronic communications.

- Online safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.
- Online safety concerns safeguarding children and young people in the digital world.
- Online safety emphasises learning to understand and use new technologies in a positive way.
- Online safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- Online safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school, and into their adult and working lives.
- Online safety Policy reflects the importance it places on the safe use of information systems and electronic communications.

Rationale

- The requirement to ensure that children and young people can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.
- A school online safety policy should help to ensure safe and appropriate use.
- Highlands School must demonstrate that it has provided the necessary safeguards to help ensure it has done everything that could reasonably be expected of it to manage and reduce these risks.

- The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.
- This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.
- The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data.
- In the case of both acts, action can only be taken over issues covered by the published behaviour policy.
- The online safety policy is to be enacted in conjunction with the most up-to-date Keeping Children Safe in Education and the information and support available in Annex D.

Highlands 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.

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

Links to other policies

This policy should be read in conjunction with other school policies that relate in some way to online safety to ensure consistency and to ensure that no aspect of safeguarding children in this area is omitted.

The online safety policy should be considered with the below policies.

- Safeguarding policy
- Behaviour policy
- Anti-Bullying policy
- Data Protection policy
- Code of Conduct
- RSE & PSHE policy
- Mental health and wellbeing policy
- AI guidance

The following guidance and legislation has been considered when writing this policy:

- Keeping children safe in education
- The online safety act 2023
- The data protection act 2018

- The education act 2011
- Teaching online safety in schools (DFE non-statutory guidance)
- Filtering and monitoring standards for schools and colleges
- Generative artificial intelligence (AI) in education

Section 2: Monitoring the effectiveness and impact of the policy

- The implementation of this online safety policy will be monitored by the school's ICT strategy manager, the senior leadership team and the governors sub committee (school priorities).
- The governor sub committee will receive once a year a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online +safety incidents).
- The online safety policy will be reviewed every two years, 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. Should serious online safety incidents take place, the following external persons / agencies should be informed: LA safeguarding officer, chair of governors, LADO, police.

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 students, parents and carers and staff

All instances of unacceptable behaviour that fall within the remit of this policy should be reported using the school's agreed systems including Bromcom for behaviour and CPOMS for safeguarding matters.

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.

Section 3: Roles and responsibilities

3.1. The Designated safeguarding lead

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’s online safety provision is also supported by the ICT strategy manager.

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 the headteacher/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).
- 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.
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Be trained in online safety issues and be aware of the potential serious safeguarding / child protection issues to arise from:
    - sharing of personal data access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying

3.2. The ICT strategy manager

The ICT strategy manager will work closely with the DSL to:

- 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 (school/local authority/MAT/external provider) 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

The ICT strategy manager is also responsible for:

- Taking day to day responsibility for online safety issues.

- Liaising with school technical staff. .
- Receiving reports of online safety incidents and creating a log of incidents related to technical issues to inform future online safety development.
- Regular monitoring of online safety incident logs.
- Regular monitoring of filtering / change control logs and for ensuring that:
    - The school's technical infrastructure is secure and is not open to misuse or malicious attack.
    - The school meets the safety technical requirements and any local authority online safety guidance that may apply.
    - Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
    - The filtering policy is applied.
- 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 the network / internet / virtual learning environment / remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be reported to the headteacher and online safety coordinators.
- Monitoring software / systems are implemented and updated as agreed with the headteacher.

3.3. 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 e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the school's priorities committee, whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of online safety governor to include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety Lead.
- Regularly receiving (collated and anonymised) reports of online safety incidents.
- Checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended.
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.
- Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

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

3.4. 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 must be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher is responsible for ensuring that the online safety co-ordinators and all other members of staff receive suitable training to enable them to carry out their online safety roles.
- 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 will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.
- The senior leadership team (SLT) 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.

3.5. Curriculum leads

Curriculum Leads will work with the DSL/ICT strategy manager to develop a planned and coordinated online safety education programme .

This will be provided through:

- The core computing curriculum.
- PHSE and RSE programmes.
- A mapped cross-curricular programme.
- Assemblies and pastoral programmes including our ‘stay-safe curriculum’.
- Relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- Any other relevant learning opportunities.

3.6. Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and 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 report any suspected serious misuse to safeguarding lead for investigation / action / sanction all digital communications with students / parents / carers should be on a professional level and only carried out using school systems.
- The online safety policy is adhered to in all aspects of the curriculum and other activities.
- Students understand and follow the online safety and acceptable use agreements.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- In all lessons where computers are available for pupil whole class use, including cover lessons, staff will use monitoring software.
- There is a zero-tolerance approach to incidents of online-bulying, sexual harassment, discrimination, hatred etc. Any such incidents must be reported in line with our safeguarding and behaviour systems.
- 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.

3.7. Students

- Are responsible for using the school digital technology systems in accordance with the student acceptable use agreement and online safety policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras.
- Will be expected to know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

3.8. Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use online services and devices in an appropriate way. The school will take every opportunity to help parents/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
- Publishing information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images, cloud services etc.
- Parents' evenings, letters, website, VLE 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 students in school.
- The safe and responsible use of their children's personal devices.

3.9. Community users

Community users who access school systems/website/learning platforms as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

3.10 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
- ICT strategy manager
- SLT
- Online safety governor
- Technical staff
- Curriculum leads for PSHE/RSE and Computing

Members of the online safety group (or other designated group) will assist 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..

Section 4: Online safety education programme

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

4.1. The curriculum

The curriculum will equip pupils with the skills to be digitally resilient and to critically evaluate content. This education will explicitly include how to:

- Identify, challenge, and report concerns related to misinformation, disinformation, and conspiracy theories.
- Develop critical thinking skills to question online narratives and sources of information.
- Understand the risks and safe boundaries associated with generative artificial intelligence (AI) tools.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways.

- A planned online safety curriculum for all year groups.
- Lessons are matched to need; are age-related and build on prior learning.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; RSE etc.
- It incorporates/makes use of relevant national initiatives and opportunities e.g. safer internet day and anti-bullying week.
- Key online safety messages reinforced as part of a planned programme of assemblies.
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Students should be helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. 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.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in supervising and monitoring the content of the websites visited.
- 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.

4.2. Staff/volunteers

All staff, including teaching, non-teaching, and volunteers, will receive annual safeguarding training which explicitly includes a focus on online safety. This training will ensure staff have an up-to-date understanding of the latest statutory guidance, including new online risks such as misinformation, disinformation, and conspiracy theories, as well as their individual and collective roles and responsibilities in relation to the school's filtering and monitoring systems.

Training will ensure the following is in place:

- 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.
- Half-termly PSHE / RSE training and CPD for all staff delivering our stay-safe curriculum.
- 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 DSL (or other nominated person will receive regular updates through attendance at external training events 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 DSL/ICT strategy lead (or other nominated person) will provide advice/guidance/training to individuals as required.

4.3. 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 or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons/inset days).

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.

4.4. 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 through our newsletter and website.
- Regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer webinars.
- High profile events / campaigns e.g. safer internet day.
- Reference to the relevant websites/publications through our newsletter and website.
- Sharing curriculum overviews through our website for all subjects.
- Open evenings/parent-facing events.

Section 5: Technology

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

5.1. Filtering and monitoring

The school maintains effective filtering and monitoring systems on its IT network and school-provided devices to prevent students and staff from accessing harmful, illegal, or inappropriate online content and to identify concerning behaviour. This system is managed in line with statutory KCSIE and DfE filtering and monitoring Standards.

Filtering and monitoring systems are designed and maintained to address not only static content but also risks related to dynamic content and technologies using generative AI.

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT service provider and is regularly reviewed 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 DSL 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 the SLT, the DSL, the ICT strategy manager and link 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.

The DFE's 'plan technology for your school service' is used to self-assess against the filtering and monitoring standards.

Filtering

- The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- Illegal content (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 DSL to breaches of the filtering policy, which are then acted upon.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- 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.

Monitoring

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

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the DSL or the ICT strategy manager.
- 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 - all concerns are logged on CPOMS and overseen by the executive safeguarding team.

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.
- 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).

5.2 Technical security

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

- Responsibility for technical security resides with SLT who may delegate activities to 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.
- The security of their username and password, including not allowing 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 systems 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.
- There is a risk-based approach to the allocation of student 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 ICT strategy manager is responsible for ensuring that all software purchased by and used by the school is adequately licensed 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.
- 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.
- 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 (where mobile devices are allowed access to school systems).
- Guest users are provided with appropriate access to school systems based on an identified risk profile.

5.3. Mobile technologies

The school does not accept responsibility for personal devices brought into school or any liability for loss, damage or malfunction following access to the network or wifi. The right to take, examine and search users' devices in the case of misuse is outlined in the behaviour policy.

School devices that are loaned to students are controlled by policies, firewalls and virus scanners and their use is monitored automatically in the same way as school based devices.

The table below summarises the use and access of portable devices in school:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Access to network servers	Yes	Yes	No	No	No	No
Wifi Internet Access	Yes	Yes	Yes	Yes*	Yes	Yes

* sixth form students computer/tablets only

5.4. School owned/provided devices

- All school devices are managed through the use of Mobile Device Management software.
- There is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed.
- Personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- The use of devices on trips/events away from school is clearly defined and expectations are well-communicated.
- Liability for damage aligns with current school policy for the replacement of equipment.
- Education is in place to support responsible use.

5.5. Personal devices

- There is a clear policy covering the use of personal mobile devices on school premises for all users
- Where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- Use of personal devices for school business is defined in the acceptable use policy and staff handbook.
- Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- The expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- Liability for loss/damage or malfunction of personal devices is clearly defined .
- There is clear advice and guidance at the point of entry for visitors to acknowledge school requirements

[1] Authorised device – purchased by the student/family through a school-organised scheme.

- Education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

5.6. Social media

These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

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

- Students are taught through the computing and PSHE/RSE curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.
- The school follows general rules on the use of social media and social networking sites in school i.e. being aware of social networking sites and how to use them in safe and productive ways.
- Ensuring students are fully aware of the school's code of conduct regarding the use of ICT and behaviour online.
- 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 students, parents and carers.
-

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
-
- Through regular safeguarding updates and CPD, all staff will be made aware of the professional risks associated with the use of personal social media and guided to ensure privacy options are active.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.
    - no reference should be made in social media to students, parents / carers or school staff
    - they do not engage in online discussion on personal matters relating to members of the school community.

Personal 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 during school hours.

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.
- 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.

Protecting professional indemnity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

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

5.7. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the anti-bullying policy, alongside our safeguarding policy.

The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made noticeably clear to students and members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Students are also educated through our ‘stay-safe’ curriculum on the dangers of internet grooming/sexting and child abuse. Using real life and scenario situations, students are guided with making responsible decisions while using digital equipment.

Students will be educated through the computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

5.8. Artificial intelligence (AI)

The school recognises the educational and safeguarding implications of Generative Artificial Intelligence (AI) and will manage its use in line with DfE guidance.

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes

that look real. The school will treat any use of AI to bully pupils in line with our behaviour policy. Students and staff will receive appropriate training and guidance on the capabilities, features, and associated risks of AI tools.

The school will establish clear policies for the safe and responsible use of AI by both pupils and staff, addressing risks such as the generation of inappropriate content, bias, data protection breaches, and academic integrity concerns.

All decisions regarding the procurement and widespread implementation of new AI technologies will involve the Designated Safeguarding Lead (DSL) and the Data Protection Officer (DPO) to ensure safeguarding and data protection compliance are met.

Please see our AI guidelines for safe, ethical and responsible use of generative AI.

5.9. Use of digital and video images

Staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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.

- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- Before photographs of students are published on the school website, social media or local press, staff must check against the list of students whose parents/carers have not given consent for the use of their image. This is held by the reprographics department.
- Photographs of students and student activity should only be made using school owned devices such as mobiles, tablets and laptop computers. Personal devices should not be used.
- 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 students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when sharing digital/video images that students are appropriately dressed.
- Students 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 this online safety policy.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are 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.
- Students' work can only be published with the permission of the learner and parents/carers.

5.10. 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 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 – ensuring that there is least risk to members of the school community, through such publications.

Section 6: Acceptable use agreements

All members of our community will be expected to read and sign the appropriate acceptable use agreement on joining the school and at times when the policy is updated.

See Appendix B

Section 7: Reporting and responding to inappropriate use

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.

Inappropriate use within a school context would be deemed to be anything which contravenes the staff or student acceptable user agreement. Breaches of the policy other than illegal incidents will be dealt with in line with the behaviour policy. These include:

- Mobile phone use (visible, using a phone or a phone rings/pings).
- Use of other non-permitted electronic devices.
- Inappropriate use of IT equipment during a lesson eg- playing games, watching videos or looking at websites not related to the lesson.
- Mobile phone, earphone or other electronic device use around the school site.
- Unkind and cruel comments towards another student.
- Refusal to hand over mobile phone, earphones or other electronic devices.
- Bringing the school into disrepute due to behaviours before or after school.
- Downloading or bringing into school pornographic material
- Malicious communication.
- Requesting/sending/sharing indecent electronic images of/from another person (or printed).
- Having indecent images of children/other students on phone or other device.
- Actions that put the health and safety of any other member of the school community at serious risk.

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 DSL, ICT strategy manager 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), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images

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

- Any concern about staff misuse will be reported to the headteacher, unless the concern involves the headteacher, in which case the complaint is referred to the Chair of Governors and the local authority designated officer (LADO).
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
  - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
  - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
  - Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by local authority
  - police involvement and/or action

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- 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.
- 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 deemed necessary.
- 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
  - students, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
  - governors, through regular safeguarding updates
  - local authority/external agencies, as relevant

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

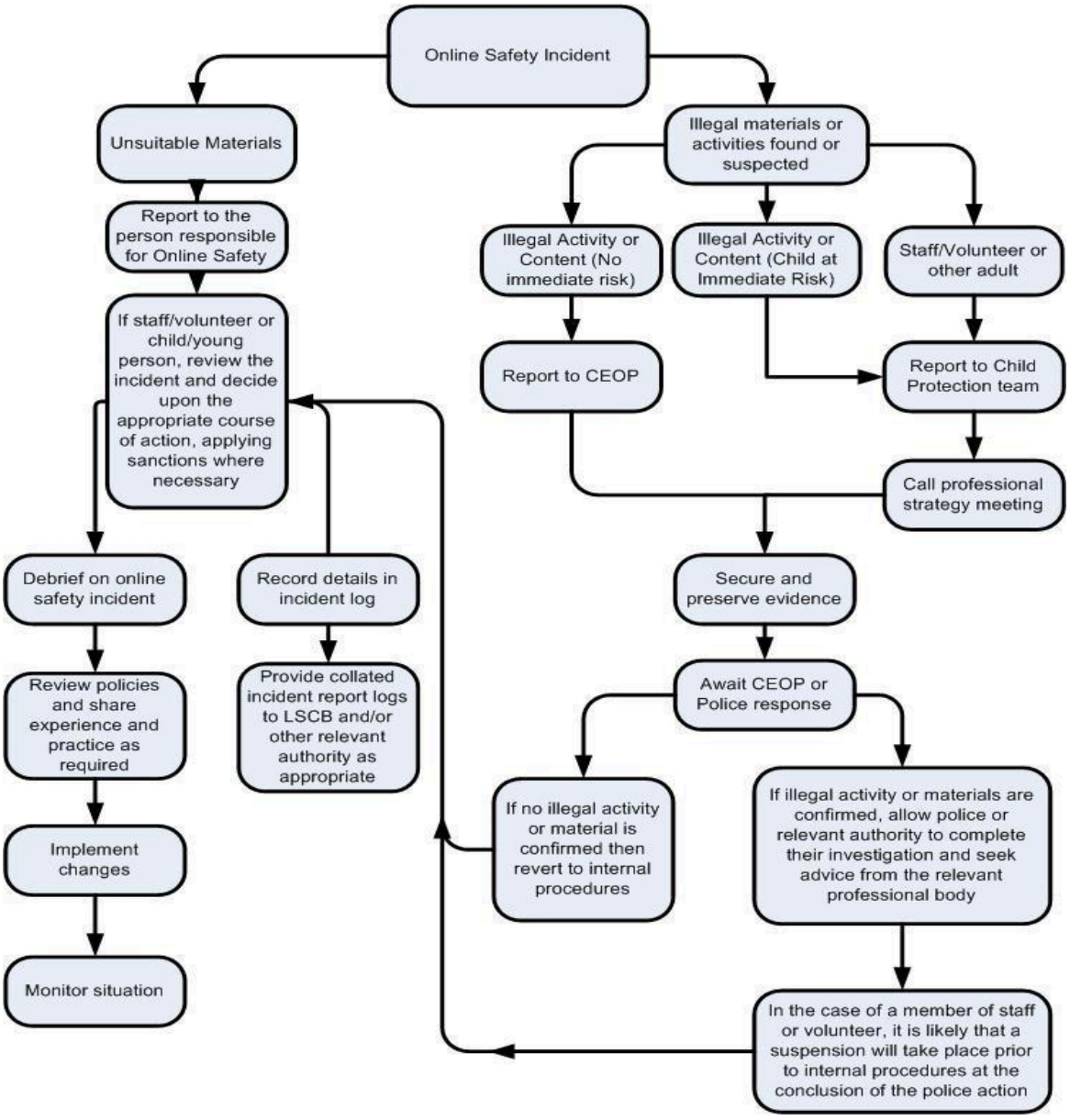
Section 8: Illegal incidents

If there is any suspicion that the activities or web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flowchart below and report immediately to the police.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the police. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Section 9: Data protection

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

The school:

- has a data protection policy.
- Implements the data protection principles and can demonstrate that it does so.
- Has paid the appropriate fee to the Information Commissioner's Office (ICO)
- Has appointed an appropriate data protection officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- 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. that of subject access which enables an individual to see/have a copy of the personal data held about them.
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data.
- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- Has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- Provides data protection training for all staff at induction and appropriate refresher training thereafter.

Staff must ensure that they:

- At all times take care to ensure the safekeeping 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.
- Will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home.
- 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.

Section 10: Communicating this policy

- This policy will be published on the school website, the staff shared network area and made available in printed form from the school office upon request.
- Staff and students will be required to sign the AUA on entry to the school and after revision of the agreement.
- Notice of any changes will be sent by email to parents, staff and students via email.

- The policy will be highlighted for students through an annual online safety week in assemblies and tutor periods.
- The acceptable use agreements will be used to highlight key responsibilities.

Appendix 1 - Acceptable Use Agreements

Highlands School

Information and Communication Technology

Acceptable Use Agreement

This form relates to the Student Acceptable Use Agreement.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

Student Agreement

I have read and understand the above and agree to follow these guidelines:

- When I use the school systems and devices (both in and out of school)
- When I use my own devices in the school (when allowed) e.g. mobile phones, USB devices, cameras etc.
- When I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school online.
- I understand that these rules are designed to keep me safe and that if they are not followed school sanctions will be applied, and my parent carer may be contacted.

Name of Student: _____Form:_____

Signed: _____Date:_____

Parent/Carer Agreement

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

- I know that my child has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed:_____ Date:_____

Student Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could compromise the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

A For my own personal safety:

1. I understand that the school will monitor my use of technology and digital communications systems provided by the school. I will not attempt to bypass the internet filtering systems.
2. I will log on to the school network with my own username and password and not allow others to know or use my network account.
3. I will be aware of "stranger danger", when I am communicating on-line. If I arrange to meet people offline that I have communicated with on-line, I will do so in a public place and take an adult with me
4. I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
5. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

B I understand that everyone has equal rights to use technology as a resource and:

1. I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
2. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
3. I will not use the school systems or devices for social media, on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

C I will act as I expect others to act toward me:

1. I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
2. I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
3. I will not take or distribute images, videos or sound files of anyone without their permission or in a manner which is designed to upset, harass or intimidate.
4. I will ensure that my online actions do not harm the reputation of the school or school community.

D I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

1. I will not alter the hardware (such as keyboards, mice or other peripheral items) and will report any observed damage, however this may have happened, to a member of staff as soon as possible.
2. I will not download or install software onto school equipment. I will not try to alter computer settings.
3. I will only use my phone in line with the school Mobile Phone Policy.
4. I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

E When using the internet for research or recreation, I recognise that:

1. I should ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not try to download copies (including music and videos)
2. When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

F I understand that I am responsible for my actions, both in and out of school:

1. I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement. This includes incidents when I am out of school and where they involve my membership of the school community (examples would be cyberbullying, use of images or personal information).
2. I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusion, contact with parents and, in the event of illegal activities, involvement of the police.

Staff, Governor and Volunteer Acceptable Use Agreement

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

A Professional and personal safety:

1. I will use the school's ICT facilities, software, hardware and any related technologies for professional purposes only and as deemed acceptable by the Head Teacher.
2. I understand that my use of ICT equipment to access the Internet and other related technologies whilst on school equipment inside or outside of the site will be monitored and logged. This can be made available, on request, to my Line Manager or Head teacher.
3. I will comply with the ICT security practices and not disclose any passwords provided to me by the school or other related authorities. I will not use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
4. I will not engage in any on-line activity that may compromise my professional responsibilities. I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
5. I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
6. I will not use a personal telephone for personal calls or texting in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room or offices.
7. I will respect copyright and intellectual property rights.

B Professional communications and actions when using school ICT systems:

8. I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner and will ensure sensitive data is sent using agreed encryption (Egress or similar).
9. I will not give out my personal details, such as mobile phone number, email address, social media accounts, to pupils and I understand that exceptions can only be given on a case by case basis by the Head Teacher.

10. I will ensure that personal data (such as data held in SIMS) is kept secure and is used appropriately, whether in school, taken off site or accessed remotely. I understand that personal data can only be taken off site or accessed remotely when authorised by the Head and that such data must be encrypted, e.g. on a password secured laptop or encrypted memory stick.
11. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
12. I will only take, store and use images of pupils or staff for professional purposes in line with school policy and with written consent of the parent, carer or staff member. I will not use my personal equipment to record these images, unless I have permission to do so.
13. I will not distribute images outside the school network without the permission of the parent/carer, member of staff or Head teacher.

C Safe and secure access to technologies and the smooth running of the school:

14. I will support and promote the school's online safety and data policies and help pupils to be safe and responsible in their use of ICT and related technologies.
15. I will always use software provided (e.g. Impero) to monitor ICT use by pupils.
16. I will not install or purchase any hardware or software for use in the school without the permission of the ICT Strategy Manager and I understand that any such permitted hardware or software may not be supported. I will not try to alter computer settings, unless this is allowed in school policies.
17. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
18. I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will immediately report any damage or faults involving equipment or software, however this may have happened.

D Responsibility for my actions in and out of the school:

19. I understand that this Acceptable Use Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and to my use of personal equipment on the premises or in situations related to my employment by the school
20. I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school information communication technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: _____ Role: Staff / Governor / Volunteer

Signed: _____ Date:_____

Appendix 2 - Remote Learning

A. During a period of remote learning due to school closures (for example COVID or adverse weather conditions) staff are required to use Google Classroom to communicate with students and to set work.

B. Guidelines for the completion of online activities, including any revised timetable or assessment schedule will be published by the senior leaders for staff to implement.

C. Students will be expected to log on, access and complete work through Google Classroom every school day.

D. Teachers will monitor and report on student activity as required as this will help students to keep up with learning and to maintain a routine that supports their well-being.

E. Meetings originating from school staff with students, parents, carers and other professionals will be conducted using Google Meet.

F. Parent Evenings held remotely will use School Cloud or a similar web based system

Guideline for periods of remote learning

1. Test your audio and video before a scheduled call.
2. Record any live classes so that the video can be reviewed if any issues arise.
3. Be punctual and courteous. Introduce yourself and take note of other attendees' names so you can address them by name. Turn off the call tone on your phone. Treat this just like you would a face to face meeting with a student, colleague or other adult.
4. Conduct yourself in a professional manner throughout the call - you remain an employee of the school throughout the call.
5. Conduct video calls to learners or colleagues from a desk or other appropriate location.
6. Remind students that all audio/video may be recorded, to safeguard both parties and this wouldn't routinely be shared.
7. Make sure to have the current client version loaded before scheduled calls.
8. Look at your screen, pay attention to others and when speaking make sure to look at your camera.
9. Use the 'blur background option' to hide any background if needed.
10. Picture in Picture is your best reference, you can see yourself and your surroundings just as others on the call can.
11. Make sure you have good light. Adjust lighting or use a portable light source to make sure you have good lighting on you from the front without having to look directly into a harsh light, eg: by pointing a strong desk lamp at the wall you're facing.
12. Ensure you are appropriately dressed; 'business casual' at all times.
13. Mute your microphone when not needing to talk to avoid background noise.
14. Keep sessions to a reasonable length and to timetabled activities.

Useful further guidance

TES: Coronavirus: 10 safeguarding rules for teachers at home

NSPCC: Undertaking remote teaching safely

NSPCC: Internet connected devices