360safe.org.uk
360safe@swgfl.org.uk

The Hub

Online Safety, Social Media and Mobile Phone usage Policy

(With appendices)

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS
Registered in England and Wales, Company Number 5589479. Charity Number 1120354. VAT Reg. Number 880 8618 88

The Hub Educational Services CIC

Online Safety Policy

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

Version: [1}

Date created: [29/09/23]

Next review date: [29/09/25]

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of The Hub Educational Services CIC to safeguard members of our community online in accordance with statutory guidance and best practice.

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

The Hub Educational Services CIC 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 the AP.

Policy development, monitoring and review

This Online Safety Policy has been developed by the whole staff.

- *Directors*
- *Designated safeguarding lead (DSL) Vanessa Brooks*
- *Online SafetyLead (OSL) Scott Brooks*
- *staff*
- *parents and carers*
- *community users*

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

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *AP on:*	*29/08/24*
The implementation of this Online Safety Policy will be monitored by:	*The Directors*
Monitoring will take place at regular intervals:	*Yearly*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Sep 2025*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Leicestershire police* *Leicestershire LADO* *Social care* *Parents*

Process for monitoring the impact of the Online Safety Policy

The AP will monitor the impact of the policy using:

- *logs of reported incidents*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as

these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[1] and groups within the school.

OSL and DSL

- The Directors has a duty of care for ensuring the safety (including online safety) of members of the 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. All devices have installed Net Nanny to further protect students whilst using our equipment.
- The DSL and OSL are made aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[2].
- The Directors are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, 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 Directors will ensure that there is a system in place to allow for monitoring and support of those in the AP who carry out the internal online safety monitoring role.
- The Directors leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead through the Net nanny information.

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."*
>
> *They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"*
>
> *They (the DSL) "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

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 lead to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual checks are carried out.
- attend relevant meetings/groups
- report regularly to Directors
- 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 on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the AP's online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the AP and beyond
- liaise with staff to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/parents/carers/learners
- 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

Teaching and support staff

Staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current AP Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they immediately report any suspected misuse or problem to *(Scott Brooks)* for investigation/action, in line with the AP's safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official AP systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in the AP (where allowed) and implement current policies regarding these devices
- in sessions where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches – Net Nanny.*
- where sessions take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of the AP and in their use of social media.

Learners

- are responsible for using the AP digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy and this includes personal devices being used in the AP
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of the AP and realise that the AP's Online Safety Policy covers their actions out of the AP, if related to their membership of the The Hub.

Parents and carers

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

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

- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the AP.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

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

Community users

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

The AP encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with others.

Professional Standards

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

Policy

Online Safety Policy

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

> **"Online safety** and the school or college's approach to it should be reflected in the child protection policy"

The AP 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 AP and how they should use this understanding to help safeguard learners in the digital world
- describes how the AP 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 Acceptable use

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

Acceptable use agreements

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

- learner induction
- staff code of conduct
- communication with parents/carers
- built into sessions
- peer support.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to the provision networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in AP policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs.				X	
	Promotion of any kind of discrimination				X	
	Using AP systems to run a private business				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the AP				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awa
Online gaming			X				X	
Online shopping/commerce		X				X		
File sharing		X					X	
Social media			X				X	
Messaging/chat			X				X	

Entertainment streaming e.g. Netflix, Disney+		X				X		
Use of video broadcasting, e.g. YouTube, Twitch, TikTok		X				X		
Mobile phones may be brought to the provision		X				X		
Use of mobile phones for learning at the provision		X				X		
Use of mobile phones in social time at provision		X				X		
Taking photos on mobile phones/cameras		X					X	
Use of other personal devices, e.g. tablets, gaming devices		X				X		
Use of personal e-mail in AP, or on APl network/wi-fi			X				X	

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

- **when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the AP.**
- **any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.** Personal e-mail addresses, text messaging or social media must not be used for these communications.
- **staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the AP and its community**
- **users should immediately report to a nominated person – in accordance with the policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.
- Photographs should be taken by the IPAD only where possible.

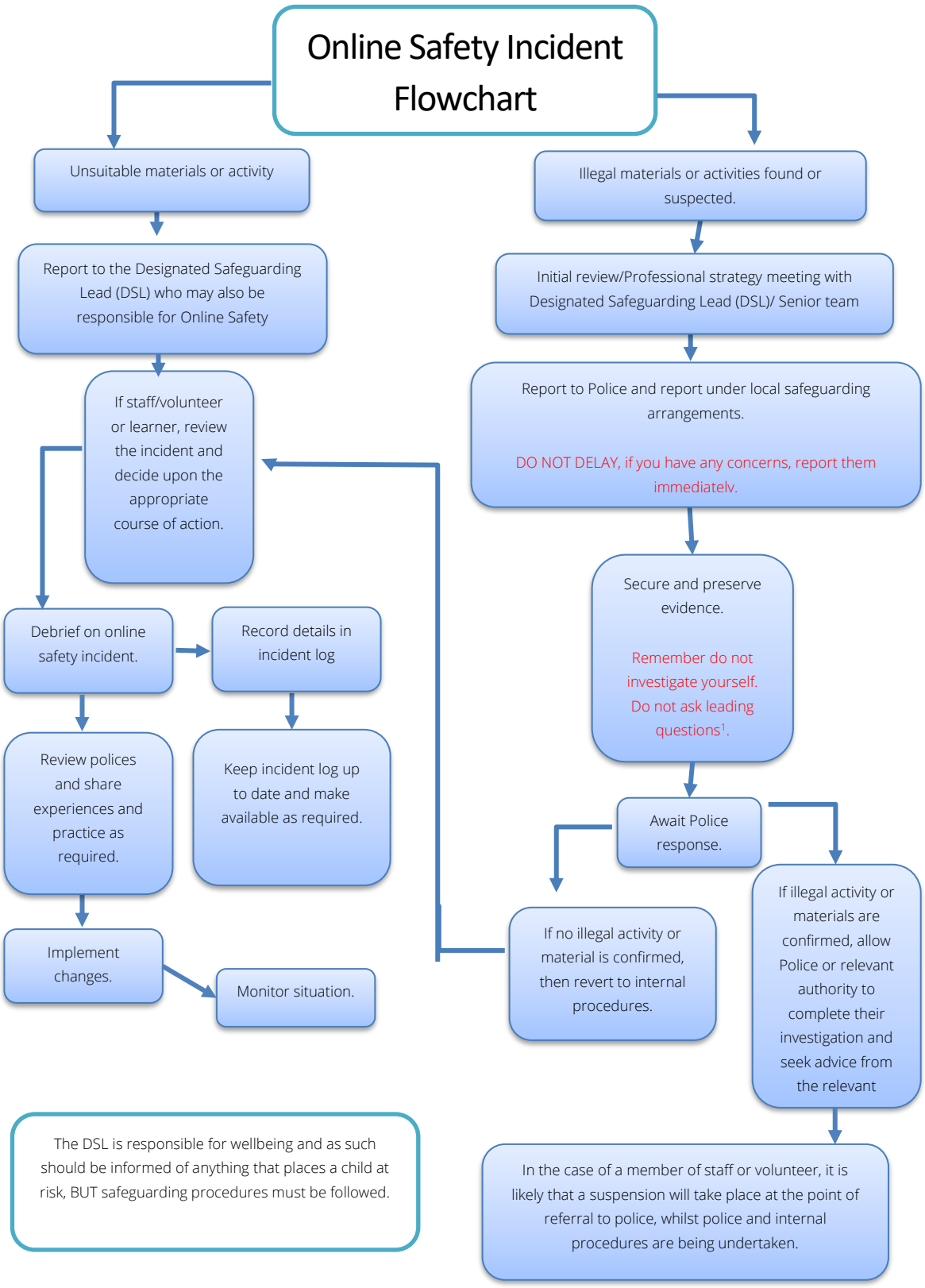
Reporting and responding

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

- **there are clear reporting routes which are understood and followed by all members of the community which are consistent with the safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**
- **all members of the community will be made aware of the need to report online safety issues/incidents**
- **reports will be dealt with as soon as is practically possible once they are received**
- **the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.**
- **if there is any suspicion that the incident involves any illegal activity or the potential for serious harm** (see flowchart and user actions chart in the appendix), **the incident must be escalated through the agreed school safeguarding procedures, this may include**
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the DSL
- 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
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
    - *staff, through regular briefings*
    - *learners, through sessions*
    - *parents/carers, through newsletters,social media, website*

Online Safety Incident Flowchart



Online Safety Education Programme

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

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

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

Keeping Children Safe in Education states:

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

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

- **A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.**
- **Lessons are matched to need; are age-related and build on prior learning**
- **Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes**
- **Learner need and progress are addressed through effective planning and assessment**
- **Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc**
- **it incorporates/makes use of relevant national initiatives and opportunities e.g.** Safer Internet Day **and** Anti-bullying week
- **the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.**
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.* Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*

- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination). Any request to do so, should be auditable, with clear reasons for the need*
- **the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.**

Contribution of Learners

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

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

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

> "All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."
>
> "Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.**"**

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

- **a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.**
- **the training will be an integral part of the AP'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 online safety policy and acceptable use agreements.**
- *the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings*
- *the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

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 AP will seek to provide information and awareness to parents and carers through:

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

Monitoring

The AP has filtering and monitoring systems in place to protect the systems and users:

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

Technical Security

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

- **all users have clearly defined access rights to AP technical systems and devices.**
- **password policy and procedures are implemented.**
- **all networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.**
- **the administrator passwords for systems are kept in a secure place**
- **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**
- **Vanessa Brooks is responsible for ensuring that all software purchased by and used by the AP 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 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**
- **staff members are not permitted to install software on a AP owned devices without the consent of the Directors**
- **removable media is not permitted unless approved**
- **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**

Mobile technologies

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

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

Mobile technology devices may be AP 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 AP's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in the AP context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the AP's online safety education programme.

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

The school allows:

	AP devices			**Personal devices**		
	AP owned for individual use	AP owned for multiple users	Authorised device[3]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes	Yes	Yes
Full wifi access	Yes	Yes	Yes	No	Yes	No

School owned/provided devices:

- *any designated mobile-free zone is clearly signposted*
- *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 the AP is clearly defined and expectation are well-communicated.*
- *liability for damage aligns with current AP policy for the replacement of equipment.*
- *education is in place to support responsible use.*

Personal devices:

- *there is a clear policy covering the use of personal mobile devices (Code of conduct)*
- *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 code of conduct.*
- *the expectations for taking/storing/using images/video aligns with the AP'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 requirements*
- *education about the safe and responsible use of mobile devices is included in the school online safety education programmes*

Social media

The AP 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, parents/carers

AP staff should ensure that:

- No reference should be made in social media to learners, parents/carers or staff.
- they do not engage in online discussion on personal matters relating to members of the community.
- personal opinions should not be attributed to the AP.
- 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 AP social media accounts are established, there should be:

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

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the AP it must be made clear that the member of staff is not communicating on behalf of the AP 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 AP are outside the scope of this policy
- where excessive personal use of social media in the AP is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of public social media

- As part of active social media engagement, the AP may pro-actively monitor the Internet for public postings about the provision.
- the AP should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the AP on social media we will urge them to make direct contact with the Hub, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the AP's complaints procedure.

Digital and video images

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

- **the AP may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.**
- **when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.**
- **staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on AP devices. The personal devices of staff should not be used for such purposes**
- *staff and volunteers are allowed to take digital/video images to support educational aims, but must follow policies concerning the sharing, storage, distribution and publication of those images*
- *care should be taken when sharing digital/video images that learners are appropriately dressed*
- *learners must not take, use, share, publish or distribute images of others without their permission*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy*
- **learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.**
- **written permission from parents or carers will be obtained before photographs of learners are taken for use in the AP or published on the AP 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 AP retention policy**
- *learners' work can only be published with the permission of the learner and parents/carers.*

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

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

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

Data Protection

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

The AP:

- **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.**
- **has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it**
- **the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed**
- **has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it**
- **information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed**
- **will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The AP '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 AP looks after their data and what their rights are**
- **has procedures in place to deal with the individual rights of the data subject,**
- **carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier**
- **has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors**
- **understands how to share data lawfully and safely with other relevant data controllers.**
- **has clear and understood policies and routines for the deletion and disposal of data**
- **reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents**

- **has a Freedom of Information Policy which sets out how it will deal with FOI requests**
- **provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff**

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

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

Staff must ensure that they:

- **at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse**
- **can recognise a possible breach, understand the need for urgency and know who to report it to within the AP**
- **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 AP**
- **only use encrypted data storage for personal data**
- **will not transfer any school personal data to personal devices**
- **use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data**
- **transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.**

Outcomes

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

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

A1 Learner Acceptable Use Agreement Template – for older learners

AP policy

Digital technologies have become integral to the lives of children and young people. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

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 AP systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *learners* to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use AP 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.

For my own personal safety:

- I understand that the AP will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to 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.
- I will be aware of "stranger danger", when I am communicating on-line.
- 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.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the AP's 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.
- 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.
- I will not use the AP's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

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

- 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.
- 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.
- I will not take or distribute images of anyone without their permission.

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

- I will only use my own personal devices (mobile phones/USB devices etc.) in The HUB if I have permission. I understand that, if I do use my own devices in the AP, I will follow the rules set out in this agreement, in the same way as if I was using AP equipment.
- I understand the risks and 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.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any AP device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

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

- 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)
- 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.

I understand that I am responsible for my actions, both in and out of The Hub:

- I understand that the AP also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the AP and where they involve my membership of the AP community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action.

Please complete the sections on the next page 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 AP systems and devices.

Learner Acceptable Use Agreement Form

This form relates to the learner acceptable use agreement; to which it is attached.

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.

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

- I use the AP's systems and devices (both in and out of school)
- I use my own devices in the AP (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the AP in a way that is related to me being a member of this AP e.g. communicating with other members of the school, accessing AP email, VLE, website etc.

Name of Learner: .....

Signed: .....

Date: .....

Parent/Carer Countersignature

A2 Learner Acceptable Use Agreement Template – for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

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

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in the AP unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of “stranger danger” when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the AP and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else’s work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.

- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/USB devices etc.) in the AP if I have permission. If I am allowed, I still have to follow all the other rules if I use them.
- I will only use social media sites with permission and at the times that are allowed
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

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

- I know that I am expected to follow these rules in the AP and that I should behave in the same way when out of The Hub as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action.

Learner Acceptable Use Agreement Form

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 AP systems.

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 The Hub)
- I use my own devices in The Hub (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of the provision and involved in any online behaviour that might affect the AP or other members of the AP.

Name of Learner: .....

Signed: ..... Date: .....

Parent/Carer Countersignature

A3 Learner Acceptable Use Agreement Template – for younger learners (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a staff member or suitable adult if I want to use the computers/tablets.
- I will only use activities that a staff member or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a staff member or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a staff member or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Signed (child): .....

Signed (parent): .....

A4 Parent/Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that AP systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- 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.

The AP will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

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

Permission Form

Parent/Carers Name: .....

Learner Name: .....

As the parent/carer of the above learners, I give permission for my son/daughter to have access to the digital technologies at the AP.

I know that my son/daughter 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 AP.

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

I understand that my son's/daughter's activity on the systems will be monitored and that the AP will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the AP if I have concerns over my child's online safety.

Signed: .....

Date: .....

A5 Staff (and Volunteer) Acceptable Use Policy Agreement Template

AP Policy

New technologies have become integral to the lives of children and young people in today's society. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

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

Acceptable Use Policy Agreement

I understand that I must use AP 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 learners 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.

For my professional and personal safety:

- I understand that the AP will monitor my use of the AP digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of the AP, and to the transfer of personal data (digital or paper based) out of the AP
- I understand that the AP digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the AP.
- I will not disclose my username or password to anyone else, nor will I try to 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.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using AP systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in The Hub in accordance with the AP's policies.
- I will only communicate with learners and parents/carers using official AP systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The AP has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the AP:

- When I use my mobile devices in The Hub, I will follow the rules set out in this agreement, in the same way as if I was using AP equipment. I will also follow any additional rules set by the AP about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the AP's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- 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.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in policies.
- I will not disable or cause any damage to AP equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for AP sanctioned personal use:

- I will 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 download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of The Hub:

- I understand that this acceptable use policy applies not only to my work and use of AP's digital technology equipment in The Hub, but also applies to my use of AP's systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the AP
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

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

Staff/Volunteer Name: .....

Signed: .....

Date: .....

A8 School Online Safety Policy Template – Harmful Sexual Behaviour

Policy for Harmful Sexual Behaviour

Statement of intent

Our Alternative Provision has a zero-tolerance approach to any harmful sexual behaviour involving children and acknowledge that it could be occurring at The Hub and in our community. The Hub is proactive in its approach to assessing prevalence, responding to incidents and challenging and changing behaviour. This policy applies to all staff and learners.

We have a statutory duty to safeguarding the children in our setting. We work together to foster an environment that creates healthy relationships for children and young people.

Our wholeapproach encourages healthy relationships and works to prevent harmful sexual behaviour. We provide high quality education within the curriculum to reduce the likelihood of the situations occurring.

We recognise that HSB is harmful to both the child/children affected by the behaviours and the child/children who displayed the behaviour and provide ongoing support for all involved.

Our approach is to treat everything as safeguarding incident in the first instance - we distinguish between behaviours that are exploratory and part of healthy age and ability appropriate development and those that may be harmful.

As a provision we provide regular opportunities for staff to understand what harmful sexual behaviours might look like and what they should do in the event of a report.

Related policies

This policy should be read in conjunction with:

- **Child protection and safeguarding policy**
- **Whistleblowing**
- **Behaviour policy**
- **Anti-bullying policy**
- **Online safety**
- **Acceptable Use Agreements**

Definitions

As stated in the Sexual Offences Act 2003, the term Harmful Sexual Behaviour (HSB) covers a wide range of behaviours, often these may be considered problematic, abusive, or violent and may also be developmentally inappropriate. HSB can occur online, offline or in a blend of both environments. The term HSB is widely acknowledged in child protection and should be treated in this context.

Whilst peer on peer harassment has become a widely recognised term, this is already moving towards child on child in recognition that age and development is a factor in making decisions about behaviour. A significant age difference between the children involved in an incident may lead to a decision about the behaviour being harmful or not. For example, this could be an older child's behaviour towards a pre-pubescent child, or a younger child's behaviour towards an older child with learning difficulties. It is important that Designated Safeguarding Leads (DSL) know what is and is not HSB. DSLs should be involved in planning the curriculum for HSB, planning preventative actions and ensuring a whole-schools culture that condones HSB, alongside all other forms of abuse and harassment. This template policy provides a basis for an effective approach to managing sexual violence and harassment.

What is sexual violence?

The following are sexual offences under the Sexual Offences Act 2003:

Rape: A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus or mouth of another person (B) with his penis, B does not consent to the penetration and A does not reasonably believe that B consents.

Assault by Penetration: A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not reasonably believe that B consents.

Sexual Assault: A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not reasonably believe that B consents. (NOTE- Schools and colleges should be aware that sexual assault covers a very wide range of behaviour so a single act of kissing someone without consent, or touching someone's bottom/breasts/genitalia without consent, can still constitute sexual assault.)

Causing someone to engage in sexual activity without consent: A person (A) commits an offence if: s/he intentionally causes another person (B) to engage in an activity, the activity is sexual, B does not consent to engaging in the activity, and A does not reasonably believe that B consents. (NOTE – this could include forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.)

What is sexual harassment?

Keeping Children Safe in Education Guidance 2022 and the Sexual Violence and sexual harassment between children in schools and colleges state:

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline and both inside and outside of school/college. When we reference sexual harassment, we do so in the context of child-on-child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names
- sexual "jokes" or taunting
- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes (schools and colleges should be considering when any of this crosses a line into sexual violence – it is important to talk to and consider the experience of the victim) and displaying pictures, photos or drawings of a sexual nature; and
- Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
- consensual and non-consensual sharing of nude and semi-nude images and/or videos. Taking and sharing nude photographs of U18s is a criminal offence.
    - sharing of unwanted explicit content
    - up skirting (this is a criminal offence)
    - sexualised online bullying.
    - unwanted sexual comments and messages, including, on social media.
    - sexual exploitation; coercion and threats.

Responsibilities

Leaders and DSLs

Our leaders and DSLs have ultimate responsibility in dealing with all incidents of harmful sexual behaviour, including online. It is the expectation that all incidents of harmful sexual behaviour/sexual violence and harassment are reported in line with school safeguarding and child protection procedures.

We ensure that our designated safeguarding lead/s (DSL) and their deputies are confident in school safeguarding processes and when it is necessary to escalate. Our DSLs know what local and national specialist support is available to support all children involved in harmful sexual behaviour and are confident as to how to access this support when required.

Designated safeguarding lead/s and their deputies have an in-depth working knowledge of key documentation, particularly KCSIE 2022 and Sexual Violence and Sexual Harassment Between Children in

Schools and Colleges (DfE 2021). We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all staff.

Staff

It is the responsibility of all staff to have read and understood this policy and associated policies. All staff must report any incidents or suspected incidents of harmful sexual behaviour to DSLs in line with school policy and ensure they are informed of the outcome. All staff will challenge any harmful sexual language or inappropriate behaviour. Staff have a duty to ensure that the environment is one which is safe and which supports learners to understand safe and healthy relationships and appropriate behaviour through delivery of our curriculum.

Learners

All learners have the right to learn in a safe, healthy and respectful school environment. Our learners benefit from a broad and balanced curriculum and are taught about healthy relationships and know how and when to report and that a range of different reporting routes is available to them. Our learners are encouraged to report any harmful sexual behaviour, even if they are not directly involved. All learners will be believed if they make a disclosure and will be treated sensitively - whilst we cannot guarantee confidentiality, their thoughts and wishes will be taken into account when supporting them.

Parents/carers

We work hard to engage parents and carers by:

- regular sessions
- sharing newsletters
- sharing information online e.g., website, social media
- providing curriculum information

Our parents and carers are made aware of how and when to report any concerns to the AP, that all incidents will be handled with care and sensitivity, and that it may sometimes be necessary to involve other agencies.

Vulnerable groups

We recognise that, nationally, vulnerable learners are three times more likely to be at risk from Harmful Sexual Behaviour. These include:

- A child with additional needs and disabilities.
- A child living with domestic abuse.
- A child who is at risk of/suffering significant harm.
- A child who is at risk of/or has been exploited or at risk of exploited (CRE, CSE),

- A care experienced child.
- A child who goes missing or is missing education.
- Children who identify as, or are perceived as, LGBTQI+ and/or any of the other protected characteristics.

Children displaying HSB have often experienced their own abuse and trauma. We ensure that any vulnerable learner is offered appropriate support, both within and outside school, sometimes via specialist agencies.

Reporting

Our systems are well promoted, easily understood and easily accessible for children and young people to confidently report abuse, knowing their concerns will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties.

Responding to an incident or disclosure

In this policy we recognise the importance of distinguishing between healthy, problematic and sexually harmful behaviour (HSB)

Our response is always based on sound safeguarding principles and follows school safeguarding processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

The AP will always adopt a multi-agency approach and seek external support and guidance, in line with policy, if deemed necessary.

Risk assessment

The AP may deem it necessary to complete a harmful sexual behaviour risk assessment as part of the response to any reported incidents. The purpose of the risk assessment is the protect and support **all those involved** by identifying potential risk, both in and out of school (e.g., including public transport, after school clubs etc) and by clearly describing the strategies put in place to mitigate such risk.

The risk assessment will be completed following a meeting with all professionals working with the learner, as well as parents or carers. Where appropriate, the learners involved will also be asked to contribute.

The risk assessment will be shared will all staff who work with the learner, as well as parents and carers. It will be dynamic and will respond to any changes in behaviour and will be regularly evaluated to assess impact.

Education

Our educational approach seeks to develop knowledge and understanding of healthy, problematic, and sexually harmful behaviours, and empowers young people to make healthy, informed decisions. Our approach is delivered predominantly through PSHE and RSE and additional opportunities are provided through:

- Cross curricular programmes (e.g., using the ProjectEVOLVE resources)
- Computing

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our setting. It is shaped and evaluated by learners and other members of the community to ensure that it is dynamic, evolving and based on need. We do this by:

- *Surveys*
- *Focus groups*
- *Parental engagement*
- *Staff consultation*
- *Staff training*

The following resources are used:

- ProjectEVOLVE - https://projectevolve.co.uk

Training

It is effective safeguarding practice for the designated safeguarding lead (and their deputies) to have a good understanding of HSB. This could form part of their safeguarding training. This will aid in planning preventative education, implementing preventative measures, drafting and implementing an effective child protection policy and incorporating the approach to sexual violence and sexual harassment into the whole approach to safeguarding.

A clear training strategy which supports staff to respond effectively to different types of harassment and sexual misconduct incidents. This should involve an assessment of the training needs of all staff. This strategy should be reviewed and evaluated on a regular basis to ensure it is fit for purpose.

Training should be made available on an ongoing basis for all staff and students to raise awareness of harassment and sexual misconduct with the purpose of preventing incidents and encouraging reporting where they do occur.

Links

Child Exploitation and Online Protection command: CEOP is a law enforcement agency which aims to keep children and young people safe from sexual exploitation and abuse. Online sexual abuse can be reported on their website and a report made to one of its Child Protection Advisors

The NSPCC provides a helpline for professionals at 0808 800 5000 and help@nspcc.org.uk. The helpline provides expert advice and support for school and college staff and will be especially useful for the designated safeguarding lead (and their deputies)

Support from specialist sexual violence sector organisations such as Rape Crisis or The Survivors Trust

The Anti-Bullying Alliance has developed guidance for schools about Sexual and sexist bullying.

The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff with regard to online safety issues

Internet Watch Foundation: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF)

Childline/IWF Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online

UKCIS Sharing nudes and semi-nudes advice: Advice for education settings working with children and young people on responding to reports of children sharing non-consensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery).

Thinkuknow from NCA-CEOP provides support for the children's workforce, parents and carers on staying safe online

Lucy Faithful Foundation

Marie Collins Foundation

NSPCC National Clinical and Assessment Service (NCATS)

Project deSHAME from Childnet provides useful research, advice and resources regarding online sexual harassment.

Date of implementation: 1/5/24

Date of next review: 1/5/25