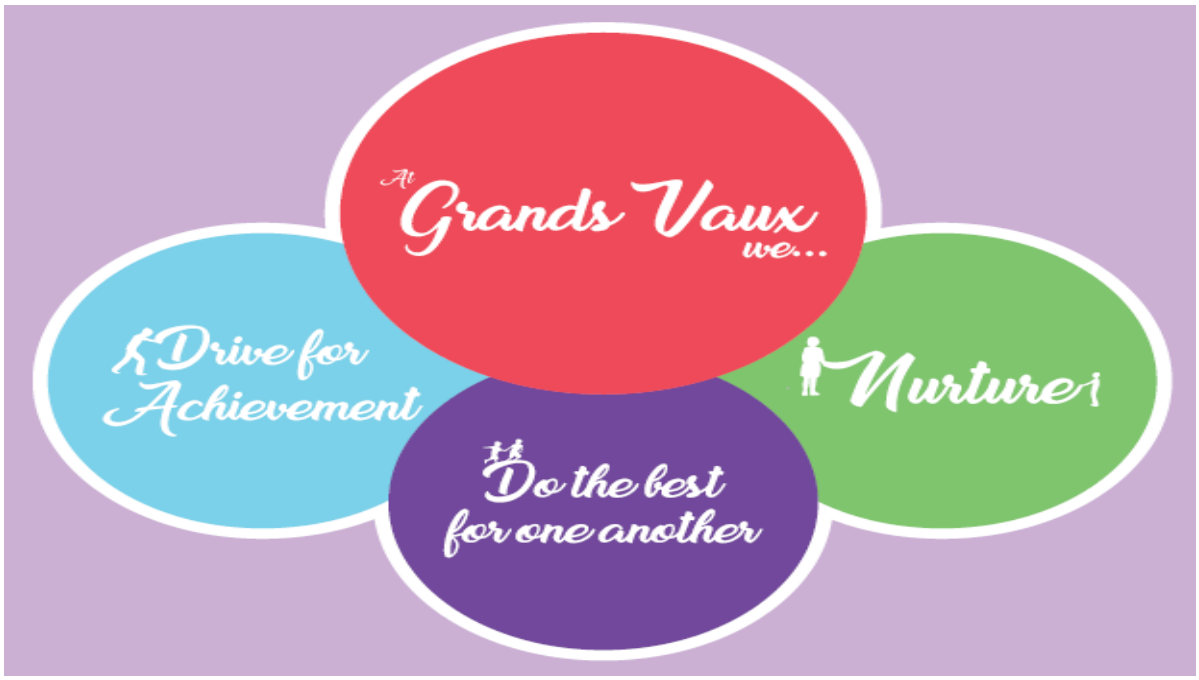
Online Safety Policy



Agreed: September 2024

Review Date: September 2025

This Online Safety Policy outlines the commitment of Grands Vaux School to safeguard members of our school community online in accordance with statutory guidance and best practice.

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

Grands Vaux 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.

As a Rights Respecting School our philosophy is underpinned by the values and principles of the United Nation's Convention on the Rights of the Child (UNCRC).

Article 3: Everyone who works with children should do what is best for each child.

Article 19: You should not be harmed and should be looked after and kept safe.

Article 36: You should be protected from doing things that could harm you.

Policy and leadership

Responsibilities

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

Headteacher 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.
- The headteacher and deputy headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (appendix 1)
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

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"

At Grands Vaux School, while the responsibility for online safety is ultimately held by the DSL (Miss McCool), we also have an Online Safety Lead to work in support of this (Miss Tanner, Deputy DSL).

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
- report regularly to leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/ /parents/carers/learners
- liaise with technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Curriculum Leads

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

This will be provided through:

- A mapped computing curriculum programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- If working remotely from home: do not divulge the password to any family members or let any member of the household use the login, laptop or device for any purpose whatsoever.
- they immediately report any suspected misuse or problem to Miss Tanner (Online Safety Lead) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media. If staff have their own social media profile we ask that profiles are not public.
- Staff will not 'friend' or accept friend requests from students on their personal social media profiles- even after they have left school.
- If parents or members of the community post negative comments about the school or staff students in the school, we DO NOT respond. Staff know to escalate this information to either Miss McCool or Ms Tanner who will then seek advice from the Head of Governance at the Department.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack

- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Miss Tanner (Online Safety Lead) or Miss McCool (DSL) for investigation and action.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

Learners

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

Parents and carers

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

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

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

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

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

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

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

Reporting and responding

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

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures (appendix 1), 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 Senior Advisor
- 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 CYPES

    - 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; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Lead for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*

The school will make the flowchart in appendix 1 available to staff to support the decision-making process for dealing with online safety incidents.

School actions

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

Online Safety Education Programme

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

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) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

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

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of school council/ /peer mediators*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

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

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

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

- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Lead and Designated Safeguarding Lead 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 Designated Safeguarding Lead/Online Safety Lead 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 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
- 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).

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

Filtering & Monitoring

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

> "It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…
>
> The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by the CYPES Department. This will remove the majority of undesirable content, but it is important to bear in mind that no filtering system is infallible, and some unpleasant content will inevitably sometimes get through. This is particularly true of image searches, where some unpleasant images are tagged with innocuous words.

As a result, all staff must ensure sufficient supervision is in place, and that as a school we develop a culture where children feel they can approach staff if they have seen anything which worries them.

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision
- 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 (Appendix 2)
- filtering logs are reviewed and alert the Designated Safeguarding Lead and Deputy DSL to breaches of the filtering policy, which are then acted upon.
- 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 – this is known as Impero. The Impero System is much a much more granular classroom management tool and allows us to see inside draft emails, and word documents. In the UK, internal school technical monitoring is a legal requirement.

The nature of this level of technical monitoring software is that there will be many 'false positives' (such as 'Moby Dick'). However, it is very important that we do not dismiss all of the flags on this basis, as some will be genuine.

Our Headteacher, Miss Maria McCool, checks our Impero database daily and responds swiftly to the email flags. She logs on to review the dashboard; reviews each category by viewing the identified captures; applies a status to each and then takes appropriate action or assigns a false positive status. Should any concern also raise safeguarding concerns this will also be logged onto MyConcern.

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

The school 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 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.

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 and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network

- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- guest users are provided with appropriate access to school systems based on an identified risk profile.

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 school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school 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 a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

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

School owned/provided devices:

- all school devices are managed though 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 expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- 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.
- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storge should be made available.
- 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
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes

Use of mobile devices

Children in year 4, 5 and 6 who walk to school are allowed to bring their mobile phones to school with them. This can help parents with peace of mind regarding their safety.

When the children arrive at school, they should hand the phone into the school office to look after for the day. These are stored in a safe place.

No member of the school community (staff, volunteers and pupils) should use their mobile phone to call, text or go online, when working with the children. Phones should be used in the staffroom or in appropriate areas where reception can be gained.

If there is any concern that there have been e-safety issues arising from the use of mobile devices, the Online Safety Officer should be made aware and will seek guidance from Lead of Governance and Risk

Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

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

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.

- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

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

Personal use

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

Monitoring of public social media

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

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

See also Social Media Policy.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital

images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

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

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- 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.
- Permission is gathered from parents or carers before photographs of learners are taken for use in school or published on the school website/social media. (Appendix 2). Permission is not required for images taken solely for internal purposes
- learners' work can only be published with the permission of the learner and parents/carers.

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters
- Seesaw

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

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

Data Protection

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 and volunteers with information about how the school looks after their data and what their rights are in a clear Privacy Notice (Appendix 3)
- 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**.**
- 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

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

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

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school

- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes

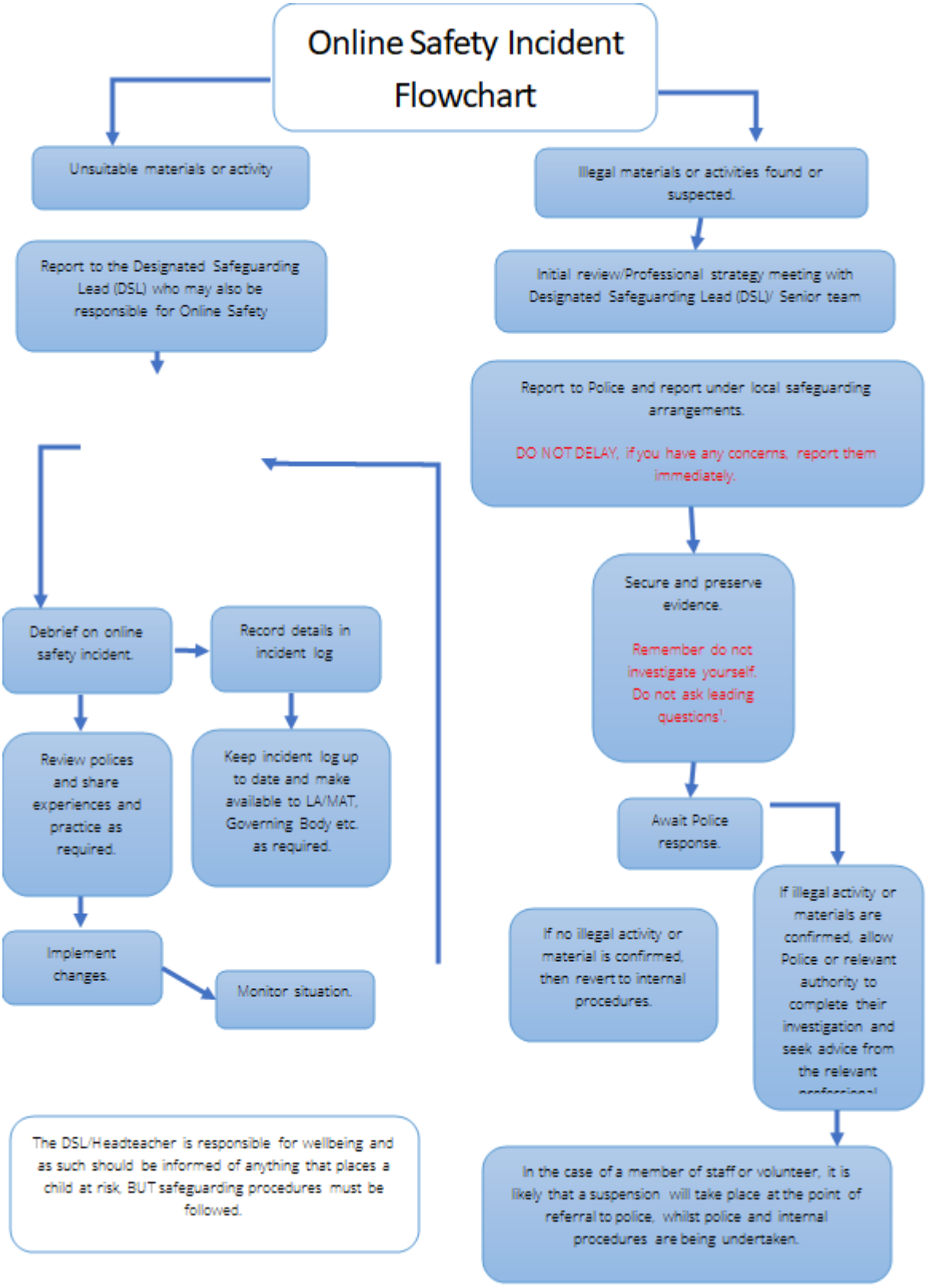
The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership
- 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

CHANGE HISTORY

Version	Date Issued	Issued by	Reason for Change	Presented To	Approved by:	Date
0.1	May 2012	Amory Charlesworth	Draft	Teaching staff	J.Hervieu	July 2012
0.2	March 2016	Lisa Harber	Review and update	Teaching Staff	J.Hervieu	March 2016
0.3	November 2018	Jamie Hazley	Updates in line with "Online Safety" policy issued by the CYPES Department in September 2018	Teaching staff		
0.4	December 2018	Jamie Hazley	Updated with Securus Software® Processes	Maria McCool		
0.5	September 2021	Jamie Hazley	Updated with Impero and additional content within the Curriculum	Maria McCool	M.McCool	Oct 21
	Oct 21	Maria McCool	Updated as above	All staff		Oct 21
0.6	Oct 22	Maria McCool	Change to staffing	Website	M.McCool	Oct 22
0.7	Oct 24	Sam Tanner	Updated	Website and all staff	M.McCool	Oct 24

Appendix 1 – Responding to incidents of misuse.



Appendix 2

GRANDS VAUX SCHOOL – PARENT CONSENT FORM

(UPDATED September 2024)

Data Protection Permissions 2018+

Grands Vaux School Jersey, is registered as a 'Controller' under the Data Protection (Jersey) Law 2018 as we collect and process personal information about you. We process and hold your information in order to provide public services and meet our statutory obligations. Please see the privacy notice on our Website (www.grandsvaux.sch.je) This notice explains how we use and share your information. Information may be collected in a paper or online form, by telephone, email, or by a member of our staff, or in some cases, by another States department. We will continually review and update this privacy notice to reflect changes in our services and feedback from service users, as well as to comply with changes in the law. The Data Protection Law is a privacy law which means that Grands Vaux School will not release your child's or your data to a third party unless a provision of the Law is met. This form should be read in conjunction with the school's latest Fair Processing Notice. There are a number of occasions when we may share your child's data with third parties and we ask you to sign this form as a record of your consent to the following disclosures.

(Tick box yes or no)	Yes	No
I give permission for my child's name, photograph and video to be used in brochures, School / Nursery handbook, displays and newsletters published by Grands Vaux School / the Government of Jersey		
I give permission for my child's name and photograph to be uploaded on Grands Vaux School website. Child's name to be mentioned but not linked to any photograph of them on the website		
I give permission for my child's photograph to be used on the school's Facebook Page.		
I give permission for my child's name, photograph and video to be used by official media (who may also use various Social Media platforms including Facebook and Twitter) when the school has asked them to record individual, class or whole school activities that are of interest to the general public eg: Jersey Evening Post Reception whole class New Starters photograph / JEP, Parish newsletter, local radio, and television broadcasters		
I give permission for my child's name to be provided to Bentley Photography to provide Grands Vaux School with a photo of my child		
I give permission for my child's name, age and work to be entered into competitions such as Jersey Eisteddfod		
I am happy for information to be shared with Grands Vaux Schools partner education services such as the Jersey Music Service and Jersey Sport		
I give permission for my child's name, date of birth and contact details to be given to the Health Department, Family Nursing and Home Care for dental, visual, weight/height check and health screening including school age immunization		
Digital technologies have become integral to the lives of children and young people, both within schools and outside school. 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 always have an entitlement to safe internet access. The school 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. I give my permission for my child's name to be uploaded to sites school deem appropriate in supporting, tracking and enhancing learning, for example Google Classroom, Seesaw, Reading Plus etc. A full list can be found on the school's privacy notice on Grands Vaux School website.		
Grands Vaux PTA is a charitable body affiliated to Grands Vaux School. The school office will on occasion email parents/carers upcoming event information on behalf of the PTA via InTouch (SIMS school email system). I agree to receive information via SIMS email regarding PTA events through the school office. For parent information. the PTA administers a Facebook/Social media page to promote their activities. The page is checked regularly to ensure comments are appropriate and do not compromise data protection, the school's, or any person's reputation.		
We believe it is an important part of children's education for them to take part in educational visits and trips and we therefore also request that you indicate your consent. I give permission for my child to take part in any educational visits and trips planned for the year group or school		
I give permission for my child to be transported by coach/minibus/car on educational visits / places of local interest		
I give permission for my child's first name to be given to parents of classmates as part of a class list to assist with writing party invitations or Christmas cards		
I give permission for my child to use i-pad/internet as per the Acceptable Users Policy		

Please be aware that if your child is taking part in any public school events, then photographs or videos may be taken by members of the audience. If you do not wish for your child to be photographed/recorded in this way, then please ensure that you formally request in writing that they do not take part in the production. Anyone taking photographs or videos are reminded that these are only for personal use and if they contain images of any other child then they must not be shared publicly on social media such as Facebook or Twitter or in any other way.

As all primary schools in Jersey, we upload children's data to the SIMS database, this includes your contact data.
It is the parent/guardian's responsibility to ensure that the contact details held by school are up to date. Please let us know immediately of any changes.

Parents/carers can withdraw consent at any time, please contact the office at admin@grandsvaux.sch.je if you wish to opt out of any of the above consents. However, if you do opt out, this may cause delays or prevent us delivering a service to you. We will always seek to comply with your request, but we may be required to hold or process your information to comply with a legal requirement.

Appendix 3 – Privacy Notice

Grands Vaux School Jersey
Privacy Notice 2024

Grands Vaux School Jersey, is registered as a 'Controller' under the Data Protection (Jersey) Law 2018 as we collect and process personal information about you. We process and hold your information in order to provide public services and meet our statutory obligations. This notice explains how we use and share your information. Information may be collected on a paper or online form, by telephone, email, or by a member of our staff, or in some cases, by another States department.

We will continually review and update this privacy notice to reflect changes in our services and feedback from service users, as well as to comply with changes in the law.

WHAT

What information do we collect about you?

We collect the following types of information about you:

- Name of child and parent / carer
- Date of birth of child
- Address of child and parent / carer
- Contact details – phone, email
- Child DOB
- Child gender
- Verification of birth (i.e. copy of birth certificate, seen not collected)
- Medical information that is relevant to child
- Parental responsibility
- Bank account details
- Social security number
- Image via CCTV operating on the outside of the school building (see CCTV Policy)

WHY

Why do we collect information about you?

We need to collect and hold information about you, in order to:

- Stay in touch with you
- Verify you are who you say you are
- Answer your query
- Handle your application
- Provide you with information you need
- Meet our statutory obligations
- Carry out the service we provide, and to monitor and improve our performance in responding to your service request
- To ensure that we meet our legal obligations
- Where necessary for our law enforcement functions
- Where necessary to protect individuals from harm or injury
- To prevent and detect crime
- To process financial transactions including grants or payment of benefits
- To allow the statistical analysis of data so we can plan the provision of services

HOW

How will we use the information about you?

We will use the information you provide in a manner that conforms to the Data Protection (Jersey) Law 2018.

We will endeavour to keep your information accurate and up to date and not keep it for longer than is necessary. In some instances the law sets the length of time information has to be kept. Please ask to see our retention schedules for more detail about how long we retain your information.

We may not be able to provide you with a service unless we have enough information or your permission to use that information.

We will not pass any personal data on to anyone outside of the States of Jersey, other than those who either process information on our behalf, or because of a legal or statutory requirement, and we will only do so, where possible, after we have ensured that sufficient steps have been taken by the recipient to protect your personal data.

We will not disclose any information that you provide 'in confidence', to anyone else without your permission, except in

the few situations where disclosure is required by law, or where we have good reason to believe that failing to share the information would put someone else at risk. You will be told about this unless there are exceptional reasons not to do so.

We do, on the odd occasion, process your information overseas using web services that are hosted outside the European Economic Area, for example Facebook. This is processed in the US, but has been approved by another competent supervisory authority under Article 40 of the GDPR or equivalent statutory provisions, together with binding and enforceable commitments of the controller and processor to apply the appropriate safeguards such as information security procedures and checks. .

We upload children's data to the MiS (Sims Database) that is hosted in the European Union. In addition, children's data may be uploaded to GL Assessments, Hodder Education, SeeSaw, Microsoft Office, Reading plus, InTouch/Outlook and EExAT. To understand how this information is processed in more detail please read Appendix A.

Data Sharing
We may need to pass your information to other States of Jersey (SOJ) departments or organisation to fulfil your request for a service. These departments are Health, Social Services, Social Security, Multi trust agencies. These departments and organisations are obliged to keep your details securely, and only use your information for the purposes of processing our service request. Please read Appendix B for a list of organisations your data is shared with and how.

We may disclose information to other departments where it is necessary, either to comply with a legal obligation, or where permitted under other legislation. Examples of this include, but are not limited to: where the disclosure is necessary for the purposes of the prevention and/or detection of crime; for the purposes of meeting statutory obligations; or to prevent risk of harm to an individual, etc.

At no time will your information be passed to organisations for marketing or sales purposes or for any commercial use without your prior express consent.

Publication of your information	E-Mails	Telephone Calls
We may need to publish your information on our website and/or in the Jersey Gazette for the following reasons: • Where we are required by law to publicise certain information, for example performance data. • In the interests of demonstrating a fair and transparent decision-making process, for example admissions process and appeals procedure. • Where we are required to provide statistical information about a group of people; although your data will be anonymised to protect your identify. • Where you have responded to a public consultation, although your comments will be anonymised to protect your identity. We will not publish any of your sensitive personal information unless there is a requirement for us to do so in order to carry out our statutory functions.	If you email us we may keep a record of your email address and a copy of the email for record keeping purposes. For security reasons we will not include any confidential information about you in any email we send to you. We would also suggest that you keep the amount of confidential information you send to us via email to a minimum or use our secure online services where possible or correspond with us by post. We will not share your email address or your email contents unless is it necessary for us to do so; either to fulfil your request for a service; to comply with a legal obligation, or where permitted under other legislation.	We do not record or monitor any telephone calls you make to us using recording equipment, although if you leave a message on our voicemail systems your message will be kept until we are able to return your call or make a note of your message. File notes of when and why you called may be taken for record keeping purposes. We will not pass on the content of your telephone calls, unless is it necessary for us to do so; either to fulfil your request for a service; to comply with a legal obligation, or where permitted under other legislation.

Your rights

You can ask us to stop processing your information	**You request that the processing of your personal data is**

You have the right to request that we stop processing your personal data in relation to any of our services. However, this may cause delays or prevent us delivering a service to you. Where possible we will seek to comply with your request but we may be required to hold or process information to comply with a legal requirement. **You can withdraw your consent to the processing of your information** In the few instances when you have given your consent to process your information, you have the right to withdraw your consent to the further processing of your personal data. However, this may cause delays or prevent us delivering a service to you. We will always seek to comply with your request but we may be required to hold or process your information in order to comply with a legal requirement. **You can ask us to correct or amend your information** You have the right to challenge the accuracy of the information we hold about you and request that it is corrected where necessary. We will seek to ensure that corrections are made not only to the data that we hold but also any data held by other organisations/parties that process data on our behalf.	**restricted** You have the right to request that we restrict the processing of your personal information. You can exercise this right in instances where you believe the information being processed in inaccurate, out of date, or there are no legitimate grounds for the processing. We will always seek to comply with your request but we may be required to continue to process your information in order to comply with a legal requirement. **You can ask us for a copy of the information we hold about you** You are legally entitled to request a list of, or a copy of any information that we hold about you. However where our records are not held in a way that easily identifies you, for example a land registry, we may not be able to provide you with a copy of your information, although we will do everything we can to comply with your request.

Complaints

You can complain to us about the way your information is being used If you have an enquiry or concern regarding the processing of your personal data please contact: Telephone: +44 (0)1534 735808 Email: admin@grandsvaux.sch.je Grands Vaux School, Les Grands Vaux, St Saviour, Jersey, JE2 7NZ	**You can also complain to the Information Commissioner about the way your information is being used** The Office of the Information Commissioner can be contacted in the following ways: Telephone: +44 (0)1534 716530 Email: enquiries@jerseyoic.org Office of the Information Commissioner 2nd Floor, 5 Castle Street, St. Helier, Jersey, JE2 3BT

Appendix 4- Further Departmental Information around Online Risks

Cyber-Bullying

Bullying is behaviour that is deliberate, repeated more than once and is designed to be hurtful. This type of behaviour can happen both on and offline (and often both), so it is crucial to consider all surrounding behaviour.

The impact of online bullying. While cyber-bullying can be an extension of face-to-face bullying, it differs in several significant ways: the invasion of home and personal space; the difficulty in controlling the scale and scope electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target is often different to 'offline' bullying.

Policies and signposts for reporting. Schools must have anti-bullying policies which articulate that participating in such activity will not be tolerated and provide clear guidance as to who a child should contact if they feel that they or someone else is being bullied.

Support for the target. The target of cyberbullying may be in need of emotional support. Key principles here include reassuring them that they have done the right thing by telling someone; recognising that it must have been difficult for them to deal with; and reiterating that no-one has a right to do that to them. Refer to any existing pastoral support/procedures for supporting those who have been bullied in the school and refer them to helpful information and resources.

Advice for the target. It is important to advise the person being bullied not to retaliate or return the message.

Replying to messages, particularly in anger, is probably just what the bully wants, and by not replying the bully may think that the target did not receive or see the message, or that they were not bothered by it. Instead, the person should keep the evidence and take it to their parent, or a member of staff Advise the pupil to think about the information they have in the public domain and where they go online. Advising the child to change their contact details, such as their Instant Messenger identity or mobile phone number, can be an effective way of stopping unwanted contact. However, it is important to be aware that some children may not want to do this and will see this as a last resort for both practical and social reasons.

Consider bystanders. In cyber-bullying, bystanders can easily become perpetrators – by passing on or showing to other images designed to humiliate, for example, or by 'liking' or commenting on a post. They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the target. It is recommended

Contain the incident. Some forms of cyberbullying involve the distribution of content or links to content, which can exacerbate, extend and prolong the bullying. It is challenging to contain this when the content may be spread across numerous sites and networks. The quickest and most effective route to getting inappropriate material taken down from the web will be to have the person who originally posted it remove it. If you know who the person responsible is, ensure that they understand why the material is hurtful and ask them to remove it. If this is unsuccessful contact the Head of Governance at the CYPES Department who will assist you in contacting the Internet Service Provider to remove the content. Involve the wider community. Schools are advised to provide parents and carers with information about cyber-bullying policies, procedures and activities, and opportunities for becoming involved.

Self-harm

Data from the National Self-harm Registry has shown that the average person-based rate of self-harm among 10-24-year-olds was 318 per 100,000. Peak rates were observed among 15–19-year-old females (564 per

100,000) and 18–22-year-old males (448 per 100,000). Between 2007 and 2017, rates of self-harm increased by 23%, with increases most pronounced in females and those aged 10-14 years. There were marked increases in specific methods of self-harm, including those associated with high lethality.

A Journal of Adolescence report, 2017 suggests the role of the Internet has a significant factor in young people self-harm. The report highlighted three sections contributing to an increase in self-harm. This included the use of the Internet for research into self-harming practices, exploring online imagery and exposure to such images and the distinct appeal of different social media platforms for young people engaging in self-harm.

There is also a phenomenon where some young people set up new ids online in order to send themselves bullying messages- a type of digital self-harm. This issue should be considered in conjunction with the Self Harm Policy.

If a young person is considering harming themselves, they may go online to search for methods. If your monitoring software flags up a term relating to self-harm, this must be responded to as a matter of urgency, in line with Child Protection procedures.

Radicalisation

Definition. Paragraph 7 of the Prevent Duty (UK Government advice for schools) defines extremism as: 'vocal opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces.'

Statutory requirements in the UK. As a result of the Counterterrorism and Security Act 2015, specified authorities (including schools) in the UK have a duty to have 'due regard to the need to prevent people from being drawn into terrorism.' This duty includes technical monitoring for signs of radicalisation.

Does this affect Jersey? Extremist groups aim to target young people who are perhaps lonely, disenfranchised and want to feel part of a community. This can happen to any child of any background, in any geographical location who is using the internet, and Jersey is not immune.

Sexting

Definition. Sexting is a term which describes the sharing of intimate images with others, using online technologies. Sexting is an increasing phenomenon among children, even of primary age.

The Law. Creating or sending an intimate photo of a minor (if reported as a complaint by the police) is technically a criminal offence, so incidents need very careful management.

Response. If a device is involved, secure it and switch it off. Seek advice and report to your designated safeguarding officer who should follow normal child protection procedures. Factors which would be taken into account in responding to sexting incidents include: the age of the person sending the photograph and the age of the person it was sent to; whether the individual was co-coerced into sending the image; to what extent the image has been shared online and whether the child is vulnerable and if there are existing concerns.

18 rated games and films

There is a growing phenomenon of children playing adult rated first-person games such as Call of Duty or Grand Theft Auto. These games contain extreme violence, sexually explicit content, images of drug taking and other adult themes. In addition, children have access to adults from all over the world via the headset and multi-player options, which creates an added risk.

Research shows that parents often buy these games for their children, so working in partnership with parents and carers is crucial in tackling this issue.

Please refer to the Data Protection Policy for related advice on this issue.

Appendix 5 – Acceptable Use Policies – Staff and Volunteer

School Policy

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open 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 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 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 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 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 school will monitor my use of the school 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, SIMs etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school 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 school.
- 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 lock any device or screen when it is left unattended.
- If working remotely from home: do not divulge the password to any family members or let any member of the household use the login, laptop or device for any purpose whatsoever.

I will be professional in my communications and actions when using school 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 school's 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 school website) 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 school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school 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. Any private social networking sites/blogs etc will not be confused with or associated with my professional role or the school.
- During the school day, staff should only check (or send) email when they are not teaching. Outside of the school day staff are free to check and read their email at any time, to suit their preferred working pattern.

- Emails sent to staff between the hours of 6:00pm and 7:00am should be limited. Staff are not expected to check or respond to emails between these times. This curfew is applied to encourage a better work-life balance and to make staff think more carefully about the emails they are sending.
- In terms of replies to both staff and parents, we expect that any emails are responded to within a 48 hour time period. It is highly inappropriate to chase someone up for a response to an email before 48 hours have elapsed. If a response is required urgently, it may be best to consider another form of contact rather than an email. Staff may not always monitor their email accounts during the school holidays, so they may not be able to respond within 48 hours.

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school 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 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 school 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 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 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 school policies.
- I will not disable or cause any damage to school 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 School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be password protected. 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 school 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.
- I will look after equipment provided by school.
- All staff school devices must be password protected.
- If a school device is lost, stolen or damaged the Computing Coordinator, ICT technician or SLT must be informed immediately. Payment for repair/replacement may be sought.
- Technology including IWBs are turned off when not in use and iPads and laptops returned to their charging stations.

When using the online systems in my professional capacity or for school 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 school:

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

Staff/Volunteer Name:

Signed: Date:

Acceptable Use Policy – Foundation Stage and KS1
Sept 2024

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher 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 teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed by class teacher to show shared with all children in class:

Signed:

Date:

AUP – Key Stage 2 children

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 school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

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 school 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 have a password to gain access to the internet and will not share it. Logging into another child's account is not allowed.
- I will log out of any school device that I am using when I have finished.
- I understand that Grands Vaux School may search a device that I am using to ensure compliance with the Acceptable Use Policy.

I will look after the devices I use, so that the school 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 not eat or drink while using a device.

I will think about how my behaviour with technology and 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:

- Mobile phones must be handed into the office at the start of the day and collected at the end of the day. It can only be switched on when I have left school site.
- 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 school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could be:
- My teacher deciding I can only use the internet if they sit next to me.
- My teacher could stop me from using technology or the internet for a period of time.
- My parents will be contacted.
- I could face suspension from school.

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 school 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 school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: Group/Class:

Signed: Date:

Acceptable Use Policy – Parent/Carer
Sept 2024

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. 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 school 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 school 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 form, so that parents/carers will be aware of the school expectations of the young people in their care.

By accepting this form, you are agreeing to the following:
As the parent/carer of a learner at Grands Vaux School, I give permission for my son/daughter to have access to the digital technologies at school.

Either: (KS2 and above)
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 school.

Or: (KS1)
I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have 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 son's/daughter'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 agreement.

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.

Please ensure that you contact school if you have any questions around this form. Children's AUP's are signed in school with the class teacher as it is then a teaching point around online safety that can be visited regularly. This document informs you that your child will be signing an AUP in school, which will be held in a locked cupboard in the school office until you child leaves Grands Vaux. If you have any questions or objections to this then you must inform us.