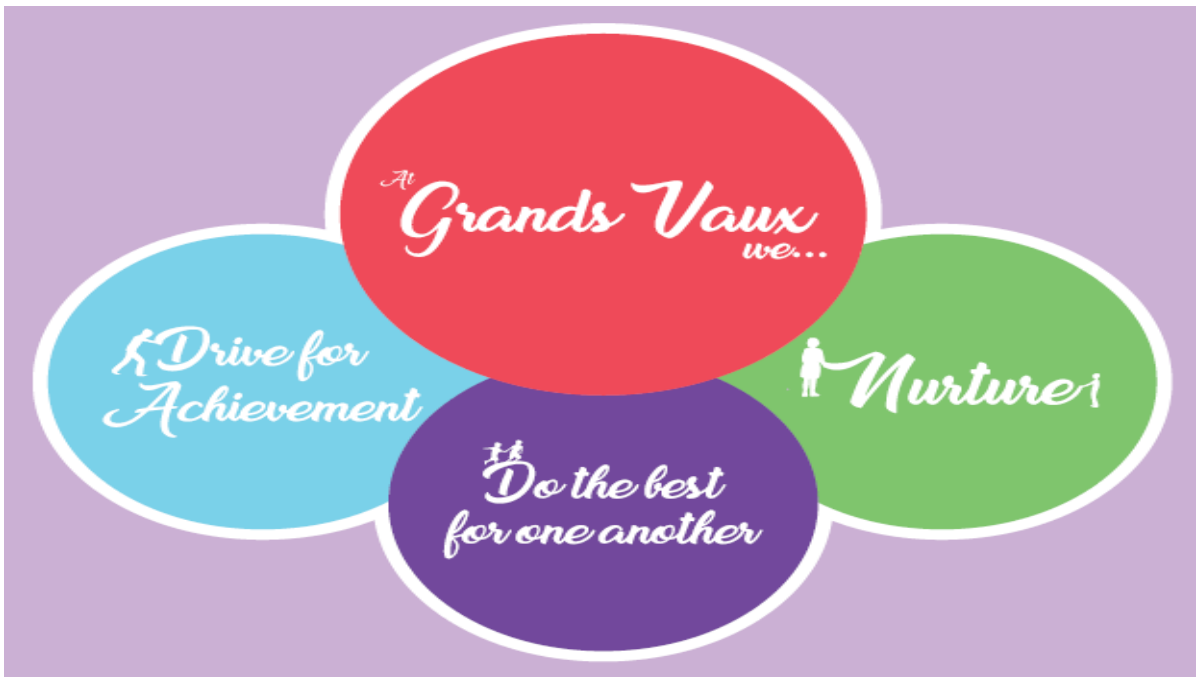
Online Safety Policy



Agreed: ……

Review Date: ……

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- ✓ Websites
- ✓ Email and Instant Messaging
- ✓ Chat Rooms and Social Networking
- ✓ Blogs
- ✓ Podcasting
- ✓ Video Broadcasting
- ✓ Downloading from the internet
- ✓ Gaming
- ✓ Mobile/Smart phones with text, video and/or web functionality
- ✓ Other mobile devices with web functionality

At Grands Vaux Primary School, we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."

Safeguarding Children in a Digital World. BECTA 2006

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.

Online Risks

The internet and constantly evolving technology have changed the way that children interact with the world. While this can offer opportunities to learn and express their creativity, this technology also offers news risks such as:

- ✓ Exposure to inappropriate material (either accidentally or deliberately)
- ✓ Cyber bullying
- ✓ Self-Harm
- ✓ Exposure to online predators
- ✓ Sexting
- ✓ Trolling
- ✓ Revealing too much personal information
- ✓ Radicalisation

Learning to recognise warning signs will allow trusted adults to intervene where appropriate and to lessen the impact of potential negative experiences. It is vital for **ALL STAFF** to stay well informed about the issues relating to what children are experiencing using social networking, webcams, blogs, instant messaging etc.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher has ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety Officer in our school is **Miss Sam Tanner**, the deputy is **Miss Maria McCool**. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety Officer to keep abreast of current issues and guidance through organisations such as CEOP.

The Online Safety Officer updates the Senior Leadership Team. The SLT understands the issues at our school in relation to local and national guidelines and advice.

Headteacher and SLT

- ✓ The Headteacher and SLT are responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- ✓ The Headteacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- ✓ The Headteacher is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- ✓ Reviews the Impero Dashboard Daily

The Online Safety Officer

- ✓ Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.

- ✓ Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- ✓ Provides training and advice for staff.
- ✓ Liaises with school Computing Technician- **Mr Paul McClemens**
- ✓ Receives daily reports of e-safety incidents (lightspeed reports) and creates a log of incidents to inform future e-safety developments.
- ✓ Monitor and promote positive online safety, through the use of *Lightspeed reports (ceased July 2021)* and currently through the Impero Package.

All School Staff

- ✓ Monitor and promote positive online safety
- ✓ Act on and escalate all online safety issues promptly and escalate to the Online Safety Officer in accordance with the Child Protection and other Safeguarding policies
- ✓ Sign an Acceptable User Agreement and adhere to the responsibilities set out therein **(See Appendix 3 for copies of both the staff and children's AUP)**
- ✓ Only use work email address to communicate
- ✓ 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; use a designated room or space to work from; keep the device locked up and secure at all times
- ✓ Use every appropriate opportunity to link online safety into the everyday curriculum
- ✓ Encrypt personal data (especially if transferring information, this should be via encrypted USB or encrypting software)- encrypted USB sticks were issued in October 2018 to all staff and a risk assessment was submitted to Alexa Munn in respect to these
- ✓ Only use websites and web-based applications with students when they have been risk assessed and you have read and reviewed the terms and conditions and are satisfied that they do not pose a significant online safety or data protection risk
- ✓ Not allow anyone else (whether children or other members of staff) to use their log on details or leave their computer or device unattended when logged into
- ✓ Not attempt to compromise or bypass online safety measures for the sake of expedience or convenience

Internet Filtering and Blocking

Light speed

Grands Vaux has internet content filtered centrally 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.

Both the Headteacher and Online Safety Officer receive daily Lightspeed reports and when there is a concerning search these are dealt with according to policy and actions taken are recorded onto the tracking grid saved in the admin shared drive. *False Positives* were not recorded.

Staff accounts have much less filtering applied than student accounts. Staff can apply for sites to be unblocked to staff accounts via the school technician and then a performa or risk assessment will be been completed.

Many digital 'apps' are able to circumvent the central monitoring and filtering so vigilant monitoring of this will be undertaken.

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.

See the **Acceptable User Policy** for guidance in acceptable use of technology in school.

Web histories

For children

For safeguarding reasons, the Online Safety Officer is able to request the web history of a child. She will request as a Helpdesk ticket - but will not name the child in the ticket and ask for a call back. The search and the reasons for the report should be documented in the child's file, and the outcome of the report integrated within any other child protection procedures.

For staff

On some occasions it will be legitimate to carry out a web history search for a member of staff. This maybe a formal request as part of a disciplinary procedure or similar. All requests should be from the Head teacher, the Police or to complete a statutory function.

If illegal content is found

If illegal or potentially illegal content is found on the schools' network or a school owned device, the machine is immediately closed down, the room or area will be secured and the advice of the Headteacher will be sought immediately. The Headteacher will then contact the Head of Governance or Head of Inclusion at the CYPES Department who will provide further advice and facilitate contact with the Police.

Do not forward, copy, print or save what you have found as this could potentially be a criminal act (i.e. making indecent images) and lead to a prosecution. The police will review the material and take appropriate action.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- ✓ The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- ✓ Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.

- ✓ Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- ✓ As part of the new Computing curriculum, all year groups have digital literacy objectives that focus on different elements of staying safe online. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- ✓ The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through computing, we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. Each class will ensure that they cover a different strand of Online Safety every half term and will take part in Safer Internet Day each year.

Through the use of the school website, parents are able to access resources that will help to support them at home by understanding the different applications and programs that their children access at home, including information about Gaming Addiction. These documents can be found at http://www.grandsvaux.sch.je/mash/.

Social Media

At Grands Vaux we recognise social media as a particular risk area for children. Unlike in recent years, where young people would be on one platform, young people use a wide variety of online platforms to share personal content. This can mean that any risk and issues are more complex.

Age restrictions. Under U.S. Law a child must be minimum age 13 to use social media platform and this message is shared with the children and parents of the school in newsletters and advice is available on the school website. Under the Data Protection 2018 Legislation, the Information Society has been introduced; this includes when offering an online service directly to a child, in the UK only children aged 13 or over are able provide their own consent.

Staff's Social Media accounts

All staff are asked to ensure that their personal Social media profiles are locked down and not publicly viewable.

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.

Published content and the school web site

The contact details on the school website are the school address, e-mail and telephone number. Staff or pupils' personal information is not published. The head teacher and Online Safety Officer take overall editorial responsibility and ensure that content is accurate and appropriate.

Written permission from parents or carers is obtained before photographs of pupils are published on the school Website. This information is stored securely on the admin drive. This consent form is considered valid for the entire period that the child attends this school unless there is a change in

the child's circumstances where consent could be an issue. **(See Appendix 2- Parental Consent Form)**

Parents/carers may withdraw permission, in writing, at any time.

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.

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 - **Mrs Alexa Munn.**

Key questions addressed by the Online Safety Officer to ensure online safety compliance

- ✓ Are you writing new and updated polices and distributing them?
- ✓ Are you involving all of your staff in online safety and training them where appropriate? Do all staff see online safety as their responsibility?
- ✓ Are you making use of filtering and monitoring software?
- ✓ Are you engaging parents, carers and the wider community?
- ✓ Are you maintaining accurate records of online safety incidents and including them on the child's file?
- ✓ Do the children in your school understand the risks around online safety and how to respond if they see anything that worries them?

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	Teaching staff		

			issued by the CYPES Department in September 2018			
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

Appendix 1- 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 2- Parental Consents Form

Grands Vaux Primary School

Headteacher: Miss Maria McCool

GRANDS VAUX SCHOOL – PARENT CONSENT FORM

(UPDATED MAY 2021)

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 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 Grand Vaux Schools partner education services such as the Jersey Music Service and Jersey Sport		
I give consent for my child's name to be uploaded to the See Saw Pupil Learning Platform to support continued learning from home.		
I give permission for my child's name, date of birth and contact details to be given to Jersey Health & Social Services Department and Family Nursing and Home Care for dental, visual, weight/height check and health screening including school age immunization		
I give permission for my child's English and Mathematics assessment data to be inputted, analysed and stored by Hodder Education Group as part of Grands Vaux's academic monitoring arrangements in Key Stage 1 & 2. I understand that this data is only accessible by staff at Grands Vaux School.		
I give permission for my child's assessment data to be processed by Early Excellence Ltd (EExAT) as part of Grands Vaux's academic monitoring and reporting arrangements in Foundation Stage. I understand that this data is only accessible by staff at Grands Vaux School and used to target children's learning and monitoring progress. It is not available to other schools or the wider community unless a child transfers to another school		
I give permission that assessment data can be processed by BSquared Ltd and/or Catch Up Maths as part of Grands Vaux academic monitoring arrangements. I understand that this data is only accessible by staff at Grands Vaux School and used to target children's learning and monitoring progress. It is not available to other schools or the wider community		
Reception to Year 6 only. I give permission for my child to use i-pad/internet as per the Acceptable Users Policy		
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 by 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 name to be given to parents of classmates as part of a class list to assist with writing party invitations or Christmas cards		

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 in order to comply with a legal requirement.

Child's Name:		Date of Birth:	
Parent/Guardian's Signature:		Year Group:	
Parent/Guardian's Full name		Date:	

Appendix 3- Acceptable User Policies- Staff and Children

Pupil Acceptable Use Policy

Grands Vaux Primary School is pleased to offer the opportunity for children across the school to be using iPads. The use of the iPad in the classroom provides an opportunity to enhance each pupil's overall learning experience. Utilising the iPads at Grands Vaux Primary School gives pupils the access to learn in a variety of ways. This learning also narrows the digital divide between pupils and promotes responsible use of today's ever changing technologies.

Please read the following User Agreement and sign at the end of the document.

School Website
The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
The publications of children's work will be decided by a teacher.
The school will endeavor to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual children will not be published on the school website without parental permission.
The school website will avoid publishing the full names of individuals in a photograph.
The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

Sanctions
Persistent misuse of the internet by pupils will result in reduced access to the Internet. Misuse of other technologies will result in a complete ban and/or confiscation.
Both of these actions will take place for a set period of time agreed by the Head Teacher.
Parents will always be notified.

Safeguarding and Maintaining as an Academic Tool
IPads belonging to the school are not to be tampered with in any manner. If an iPad is found unattended, it should be given to the nearest member of staff. The iPad is an instructional tool and must be treated as such. Pupils may not use the iPad for non-academic purposes during school hours.

Care and Use of iPad
The iPads are the property of Grands Vaux Primary School and will be check by staff members at Grands Vaux Primary School;

Pupils may not download any content to the iPad using a personal iTunes account;

Pupils may not make chanegs to the iPads (Backgrounds/wallpaper etc...);

Pupils will be given a password to gain access to the internet. Pupils are responsible for remembering this password and not sharing it with others;

Logging into another pupil's internet account is prohibited;

Pupils will not use the Internet to download music, pictures, or any other files without permission from the classroom Teacher;

Pupils may not alter the profile on any iPad owned by Grands Vaux Primary School;

IPads must be kept away from liquids and food - do not eat or drink while using the iPad;

Care must be kept to keep the iPad from being damaged;

The iPad must always remain in the school's purchased case;

All users have a responsibility to report any known misuses of technology, including the unacceptable behaviors of others.

Prohibited Uses Include:
Accessing Inappropriate Materials - Pupils are not allowed to send, access, upload, download, or distribute inappropriate materials.
Cameras - Pupils must use good judgment when using the camera. The pupil agrees that the camera will not be used to take inappropriate photographs or videos, nor will it be used to embarrass anyone in any way.
Malicious Use/Vandalism - Any attempt to destroy hardware, software or data will result in that pupil being prohibited from using the iPad in the future.
E-Safety
Grands Vaux Primary School provides a high level of internet content filtering on our wireless network. Pupil use of the Internet during school hours is monitored by adults.

Grands Vaux Primary School reserves the right to search an iPad that is currently being used by a pupil to ensure compliance with the Acceptable Use Policy. Pupils in breach of the Acceptable Use Policy may be subject to disciplinary action.

Pupil Consent

I know that if I break these rules then these could happen:

- I could put myself or others in danger.
- My teacher could decide that I only use the internet if they sit next to me.
- My teacher could stop me from using technology or the internet for a time.
- My parents will be contacted.

I have read and agree to follow these rules:

Name:_____ Signed: _____

Parent Consent

I have read and understood the school rules for responsible internet use and give permission for my son or daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:_____ Date:_____

Please print name: _____

Staff Acceptable Use Policy

Grands Vaux Primary School is pleased to offer the opportunity for staff across the school to be using iPads. The use of the iPad in the classroom provides an opportunity to enhance each pupil's overall learning experience. Utilising the iPads at Grands Vaux Primary School gives staff the access to teach in a variety of ways. This teaching also narrows the digital divide between pupils and promotes responsible use of today's ever changing technologies.

Please read the following User Agreement and sign at the end of the document.

I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head Teacher.
I will not reveal my password(s) to anyone.
I will not allow unauthorized individuals to access email / Internet / intranet / network, or other school systems.
I will not engage in any online activity that may compromise my professional responsibilities.
I will only use the approved, secure email system for any school business.
I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
I will not browse, download or send material that could be considered offensive to colleagues.
I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
I will not connect a computer, laptop or other device, to the network / Internet that does not have up-to-date anti-virus software.
I will not use personal digital cameras or any device with camera capabilities for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
Staff iPads will only be used as an educational tool. Any inappropriate use of the iPad will be reported to the Deputy Head Teacher or the Head Teacher. This will be reviewed with the member of staff involved.
Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use.
I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with or associated with my professional role or the school.
I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
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.
This is a professional environment, and as such, we expect all emails to be written in a professional manner and using correct language.
With email often being our first point of contact with outside agencies, it is vital we present ourselves as well as we can. As staff at a school, we are expected to have a good knowledge of the English language and spelling. Therefore we expect some effort to be made to email using correct grammar, punctuation and spelling, especially when interacting with parents or outside individuals.
I understand that failure to comply with this agreement could lead to disciplinary action.

Safeguarding and Maintaining as an Academic Tool
IPads belonging to the school are not to be tampered with in any manner. If an iPad is found unattended, it should be given to the nearest member of staff as soon as possible. The iPad is an educational tool and must be treated as such.

Care and Use of iPad
The iPad screen is made of glass and is therefore subject to cracking and breaking if misused; never drop or place heavy objects (book, laptops etc.) on top of the iPad.
Do not leave the iPad unattended and the whereabouts of the iPad should be known at all times.
Images of other people may only be made with the permission of the person, or parents of the person, in the photograph.
Upon returning the iPad to the school, it is the user's responsibility to delete all personal materials, including pictures, passwords and e-mails from the device.
If the iPad is lost, stolen or damaged, the Computing Coordinator, ICT Technician, Deputy Head Teacher or Head Teacher must be informed immediately and payment agreed.

Prohibited Uses Include:
Accessing Inappropriate Materials - Staff are not allowed to send, access, upload, download, or distribute inappropriate materials.
Malicious Use*/*Vandalism - Any attempt to destroy hardware, software or data.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies and I agree to abide by all the points above.

I wish to have an email account; be connected to the Internet; be able to use the school's ICT resources and systems.

Signature …… Date: …….

Full Name ..... (printed)

Job title .....