Grouville School Digital Safeguarding Policy 2020

Well-being and achievement are at the heart of Grouville School so that we can all develop as Lifelong Learners and take responsibility for ourselves and the community.

Article 13: *Every child must be free to say what they think and to seek and receive all kinds of information, as long as it is within the law.* ***Article 16:*** *Every child has the right to privacy.* ***Article 17:*** *Every child has the right to reliable information from the media.* ***Article 28:*** *Every child has the right to an education.* ***Article 29:*** *Education must develop every child's personality, talents and abilities to the full.* ***Article 34:*** *Governments must protect children from sexual abuse and exploitation.* ***Article 36:*** *Governments must protect children from all other forms of bad treatment.*

Linked Policies

- Child Protection & Safeguarding
- Data Protection
- Behaviour
- Counterbullying
- Social Media
- Computing

Overview

At Grouville, we are committed to providing outstanding learning experiences for our children. Our use of technology underpins, supports, extends, engages and enriches our children's learning experiences. (See Computing Policy)

This Digital Safeguarding Policy outlines our safety expectations in respect of all technological devices including fixed and mobile devices. It will be revised to incorporate new and emerging technologies. As our digital resources grow, so has the awareness of risks and potential dangers, which arise from their use. We aim to prepare our children with the knowledge and ability to make informed, safe decisions online and therefore allow them to thrive in our ever-developing digital world.

As a school it is our duty of care, alongside that of parents, and other members of the community to protect our children from harm online and using technology. The purpose of our Digital Safeguarding Policy is to outline what measures Grouville School takes to ensure that children can work in a safe environment and to outline reporting procedures for safety concerns.

Scope of the Policy:

This policy applies to all members of the school community including staff, children and parents who have access to, and are users of school ICT systems, both in and out of Grouville. The terms 'online safety' and 'digital safeguarding' are interchangeable for the purpose of this policy. This policy will form part with our school safeguarding policy and will form close links to other policies listed above All incidents will be dealt with appropriately and staff will be expected to follow the procedures outlined in this policy to ensure the safety of the children in our school.

Management of Digital Safeguarding

All staff are responsible for safeguarding our children in a digital environment. Staff will take part in online safety training opportunities and will be actively supported by the Digital Safeguarding Leader (DSL) and the Child Protection Officers (CPO) to ensure suitable procedures are in place. Teachers have a responsibility to cover the expected Digital Literacy element of the Computing Curriculum as required for their specific Year Group.

Roles and Responsibilities

Child Protection Officers (CPO):

- are responsible for the duty of care and safety (including online) of members of the school community, though the day-to-day responsibility for online safety is delegated to the DSL, supported by SLT.
- will lead procedures in the event of a serious online safety concern or allegation regarding staff, children or parents. Procedures for serious concerns will follow those outlined in the Child Protection & Safeguarding Policy. SLT (including DSL) will lead in their absence.
- are responsible for ensuring that all members staff receive suitable safety (including online safety) training to enable them to carry out their roles effectively.
- will receive weekly updates from the DSL, if necessary, to ensure safety and training meets the school needs and to be informed of any relevant incidents that arise.

Digital Safeguarding Leader (DSL) will:

- take responsibility for monitoring and reporting daily digital safeguarding issues.
- create and review the school Digital Safeguarding Policy.
- ensure that all staff understand and follow the reporting procedures in the event of a digital safeguarding incident (Appendix 1).
- attend and complete training opportunities to ensure digital safeguarding at Grouville School is in keeping with current movements in technology.
- provide and organise training for all staff at Grouville School and extend these opportunities to our parental community including formal training requirements outlined by CPOs.
- liaise with The Education Department teams to ensure Grouville School's digital safeguarding practice reflects developments Island-wide.
- receive and review all digital safeguarding incident logs to inform future digital safeguarding developments and actions for individuals and larger cohorts of children.
- report key developments and issues to the SLT.
- complete risk assessments for all online services and apps that require data sharing.

Staff will:

- read and adhere to the Staff Responsible User Agreement (Appendix 2).
- follow the technology incident reporting guidelines (Appendix 1) to report or deal with any suspected misuse, or online safety issues.
- ensure all digital communications with children & parents about school is on a professional level and only carried out using official school systems.
- ensure children understand and follow the relevant Responsible Use Agreements.
- ensure children hand in mobile technology to the office storage box at the beginning of each day-turned off and to monitor these rules at key times such as morning drop off/collection.
- monitor the use of technology throughout the school day to ensure children are digitally safe.
- not register, use or send data online using services that haven't been risk assessed or approved by Grouville School. (See Data Protection Policy).
- check suitability of online resources and apps before use.
- keep all personal login information private.
- Teachers will deliver the Digital Literacy element of the Computing Curriculum and will reinforce online safety across the curriculum where relevant. (See Computing Policy)

Children will:

- read and sign the age-related Responsible Use Agreement and follow the expectations outlined.
- not use home devices (BYOD) at school unless they have been granted special permission to do so.
- hand in all devices including mobile phones, switched off, to the office at the beginning of each day and keep them turned off and out of sight until off school property.
- know how to report incidents to members of staff in school and to trusted adults outside of school hours.
- Respect personal privacy and keep their own and other people's personal information private, including photographs and passwords.
- Behave in a respectful, responsible and safe manner towards digital technologies and when engaging in online activities at school and home.

Parents will:

- Sign and discuss the age-related Responsible Use Agreement with their child and discuss its implications and rules to follow at school and aspects to consider at home.
- Respect relevant policies when taking images and videos at school events. (see Social Media Policy)
- Respect school passwords and encourage their child never to attempt to obtain or to use another child's or an adult's password.
- Take a key role at home at developing their child's digital safety by proactively supervising and monitoring their child's use of technology for all primary-aged children.
- Actively monitor and discourage the use of age-inappropriate apps and online services including gaming and social media sites.

Grouville School will seek to provide information and awareness to parents and carers through:

- Clear online safety advice on our Grouville website and Facebook page.
- Letters, newsletters and information.
- High profile events & campaigns e.g. Safer Internet Day.

Infrastructure & Monitoring

Whilst technical supervision, monitoring and regulation is very important in creating a safe online environment for our children, this must be balanced by educating our children how to use online services safely and sensibly, including knowing how and who to report online issues or concerns to. The education of our children at Grouville is therefore crucial and forms an essential part of the school's safeguarding provision.

Currently, our school network infrastructure and filtering system (Lightspeed) is managed externally by The Education Department. We also hold the license for Impero – our own school filtering and monitoring system which is monitored daily by our IT Technician and DSL.

Our Computing Leader (supported by the IT Technician) is responsible for ensuring that software licences are accurate and up to date. All users are provided with a username and secure password by the ICT Technician issued by The Education Department. Users are responsible and accountable for the security of their username and password.

Data Protection (see Data Protection Policy)

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

All online services that include the transfer of personal data of our members of staff or children are risk assessed by the Digital Safeguarding Leader & supported by ICT Technician in keeping with the requirements of The Education Department's format (Appendix 6) and Jersey Law requirements. Any online service that requires the transfer of child personal data must meet the requirements of the risk assessment. No sensitive data will be transferred unless this has been elevated to the approval of the Headteacher and the Island's Data Protection Commissioner.

All online services that Grouville School currently use are outlined on our School website (as a working document) and are referenced to in our Fair Processing Statement. A consent form is signed by all parents at the beginning of each academic year and therefore should an online service be added mid-year, parents will be notified of any changes.

Images (See Social Media Policy)

The development of digital imaging technologies has created significant benefits to learning. However, staff, parents and children need to be aware of the risks associated with publishing digital images on the internet. Staff and volunteers are permitted to take digital images & video clips to support educational aims, but they must follow the below procedures regarding the sharing, distribution and publication of such images to adhere to our safeguarding aims.

- Images should only be taken on school equipment- personal equipment of staff should not be used for such purposes.
- Images must only be published and uploaded within the agreed school platforms that have been securely risk assessed.
- Written permission from parents must be obtained through the agreed school consent form before photographs of children are published on the school website, or via social media.
- No names will accompany photos of children online apart from those with escalated levels of sensitive data approval (SIMS & Provision Map).
- Care should be taken when taking digital & video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Children must not publish or distribute any images taken on school property on their own personal social media.

Staff Use of Social Media (See Social Media Policy)

Although social media is used as a personal forum, staff must be aware of protecting their professional identities through acting and posting responsibly online:

- Pictures taken on school property must not be uploaded to personal social media accounts without the permission of the Headteacher. No photos of children, personal or sensitive data present in the background should be added under any circumstances.
- Staff will ensure professional boundaries exist between staff, parents and children by:
    - Not allowing a staff network login to be used by a child.
    - Only contacting parents through the agreed school systems and procedures.
    - Not becoming 'friends' with current children, or parents (unless already known on a personal capacity) on any social networking site.

Mobile Phones & BYOD (Bring your own device)

We understand that mobile phones have become a vital communication tool between families, and that some children will have a mobile phone of their own. Some parents may feel the need for their child to carry a mobile phone with them as a safety precaution – should they be travelling to, or from school independently, or staying away from home. Whilst we recognise that every family is different, the following procedures are in place to ensure the safety of our pupils.

Pupils

- We do not support the use of BYOD at this time and personal devices (apart from mobile phones) should not be brought to school. In the rare event that a child will need to bring a device to school, it should be handed in to the office mobile phone box on arrival. Devices can be collected at the end of the day.
- Pupils are not permitted to use mobile phones at school or on trips.
- Mobile phones brought to school are left at the owner's risk and the school will not take responsibility for lost or stolen phones.
- Mobile phones that are brought to school without meeting the above criteria will be confiscated and parents will be informed.

Staff

- Staff must have their phones on 'silent' or switched off during class time and stored away from children at all times.
- Staff are not permitted to make, receive calls or send or receive texts during contact time with children.
- In emergency circumstances, staff members may request to keep their phones nearby. They must inform the Headship team or their Phase Leader before they do so for safeguarding purposes.
- Phones are brought onto the premises at personal risk and are not covered by the school insurance.
- School technology will be used to take photographs of children- the use of cameras on mobile phones should be avoided for safeguarding purposes.
- An emergency mobile phone should be taken to sporting fixtures or offsite visits for emergency contact. Staff should always hide their caller ID if calling parents from personal devices to avoid sharing personal data.
- Staff mobile numbers should be kept centrally in the event of an emergency, or of an unplanned school closure (snow closure). In that situation the Headteacher and Senior Leadership Team will communicate with staff via telephone tree to pass on key messages.

Parents, Carers & Visitors (See Social Media Policy)

- Photographs may be taken during an assembly or show, however parents must respect the school Social Media Policy and understand that photos (apart from those of their own child) must not be added to any social media platform.
- Mobile phones belonging to the general public must never be used to take photographs of the school building or grounds without due reason. It is the duty of all staff to challenge anyone who is seen doing this and report immediately to the CPOs or SLT.

D.Buesnel (Digital Safeguarding Leader)
To be reviewed in 2022

APPENDICES

Appendix 1: Guidelines for reporting Digital Safeguarding Issues

Appendix 2: Staff Responsible Use Agreement

Appendix 3: Key Stage 1 & EYFS RUA

Appendix 4: Lower KS2 RUA

Appendix 5: Upper KS2 RUA

Appendix 6: Data Protection Risk Assessment Template

Appendix 1

Responding to Online/Technology Incidents

This guidance is intended for use when staff need to manage online safety incidents. It encourages a safe, secure and consistent approach to the management of online incidents. Incidents might involve illegal or inappropriate activities.

Illegal Incidents: If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) and report immediately to Headship team using a Cause for Concern form.

An online issue is identified or reported.
Is the material accessed or the actions illegal?

NO

All Staff:

- Ask child to turn off screen.
- Address behaviour – what happened?

If accidental issue (inappropriate picture pops up etc.)

- Assess the risk.
- Debrief child with online safety message – Thank you for reporting this to me, you have done the right thing.
- Contact parent if necessary – teacher discretion.
- Email Digital Safeguarding Lead to inform.

If purposeful breach (unsafe searching, inappropriate language typed in on purpose etc.)

- Assess the risk.
- Debrief child using Behaviour Policy
- Refer to RUA (all children have signed one).
- Class teacher to log incident with Technician/Digital Safeguarding Leader.
- Contact parent.

Digital Safeguarding Leader:

Depending on the severity of the risk, the following responses may be appropriate:

- Website containing the material are blocked.
- The parents of the child may be notified
- Warnings are given to the child, if appropriate and blocking of accounts may be actioned.
- Whole-class/or one-one discussions delivered by Digital Safeguarding Leader

**Seek advice from Digital Safeguarding Leader if unsure of appropriate action.*

Following the incident…

- All incidents will be compiled into an incident log. This will inform changes to school policies in order to minimise the chances of the same online issue recurring.
- External agencies will be involved if necessary.

YES

All Staff:

If child faces an immediate risk:

- Follow Child Protection Policy Reporting Procedures.
- Reassure child-debrief child protection reporting messages.
- Contact the Headship team.
- Secure all available evidence.
- Isolate the computer in question as best you can. (Do not print, email or share any compromising information.
- Jot down web address or immediate details on a cause for concern form.
- External support to be contacted by Headship (MASH).

If the child <u>does not</u> face immediate risk:

- Contact the Headship team
- Secure all available evidence
- Reassure child-debrief child protection reporting messages.

Are illegal materials confirmed by relevant authority?

YES: Headship/SLT/Teacher to follow MASH advice and Child Protection Policy procedures.

NO: Continue to monitor the situation for any potential developments/recurrences - especially pertinent in cases of cyber bullying. Follow child protection response procedures.

Appendix 2

Staff Responsible Use Agreement

The Staff Responsible User Agreement refers to all school owned and personal devices that are being used on school premises. All staff must adhere to this user agreement to ensure the safety of themselves, the children and our school infrastructure.

Please read the information carefully below. Signed acceptance is not required: on-site use will be evidence of acceptance. All staff must act accordingly to avoid devices from being revoked from use.

1. **The user and devices**

   I understand that…

   a. All school purchased technology is owned by Grouville and should remain on site at all times, with the exception of staff iPads which can be taken home when necessary.
   b. All school-owned technology is covered by school insurance, however if users take staff iPads off-island for personal use, personal insurance will be required for any damage/loss caused.
   c. Users are responsible for the safe use of technology – charging & storing devices responsibly following our school Health & Safety procedures. Wires & plugs must be safely positioned to avoid accidents and turned off when not in use. Only authentic cables are permitted to be used for school-owned devices.
   d. iPads must be stored in lockable cabinets during holiday periods.
   e. Staff iPads are for the sole use of the Teacher or TA working alongside children within the class. They are not to be accessed or used by children for any activity.

2. **Purpose**

   I understand that…

   a. The desire to use hardwired and mobile devices at Grouville School is driven by the ambition to enhance teaching and learning.
   b. All content/data stored on staff iPads will be safe, appropriate and suitable within a primary school environment. If content is deemed to be inappropriate, the user devices may be revoked and further investigation may be required to take place.
   c. Personal devices including data access may be used on-site for personal uses only, where and when it is appropriate and permitted to do so- (breaktimes/lunchtimes with no children present).

3. **Connectivity**

   I understand that…

   a. Mobile devices must only connect to the school's network via approved routes- via Wi-Fi, Apple TV or manual port connection.
   b. Users will not share their own or use other users' login details.
   c. All content assessed through personal data internet connection must be safe, appropriate and acceptable for a primary school environment.
   d. Children do not have access to personal data internet devices on school property at this stage of our IT development. Should children bring such devices to school – mobile phones, tablets etc. these must be turned off and stored in the office storage box.
   e. The use of Grouville's network is actively monitored and that by connecting to such networks users give consent for monitoring of such use to take place.

f. Devices that are found to be compromised in any way may be denied access to the school's network (denial of access may be triggered automatically by the web filter or through manual suspension)

4. Software/apps

I understand that…

a. Users are not permitted to download or install software or hardware to the school network and all installation requests must be made to the ICT Technician or Computing Leader.
b. Many online services and apps may not be suitable for school based on Data Protection requirements and all users must consult the Computing Leader prior to purchasing any software/service so that it can be suitably risk assessed.
c. Grouville will purchase the educational apps that are installed on school iPads through the use of an outlined MDM by The Education Department.

5. Data protection

I understand that…

a. All personal data must be appropriately safeguarded on devices and at all times. A unique and secure passcode must be turned on, at all times, with further password protected apps that contain personal or sensitive data.
b. All personal data that is processed in a professional capacity may only be stored on web-based (cloud) services that have passed our Grouville School risk assessments.
c. All school owned devices are monitored and so content is not guaranteed to be private. Administrators and The Education Department have access to all computer documents and all activity is monitored.
d. All files and folders that contain personal and sensitive data must be password encrypted on mobile devices/USBs at all times.
e. Users must password protect any personal/sensitive data via email.
f. Users should never send personal or sensitive data via unprotected non-school related communication e.g. personal email addresses.

6. Security and virus protection

I understand that…

a. All mobile devices (both school-owned and personal devices) that are used professionally by members of staff must be protected, by passwords or passcodes. (see point 5a)
b. School-owned devices must be maintained in their supplied state: they must not be "jailbroken" or "rooted".
c. MDM supervision must be installed by the ICT Technician to ensure all iPads can be tracked and locked should they be lost, stolen or misplaced.
d. Users are responsible to regularly update their staff iPads to ensure the most recent updates are active and current. The ICT Technician is responsible for all other update maintenance.
e. In the event of iPads or devices being lost, users must inform the Computing Leader as quickly as is reasonably possible. Lost school-owned devices will be locked of all data centrally: the user must be aware that this may wipe all stored information.

7. Right of Inspection

I understand that…

a. The on-site use of all mobile devices, both home-owned and school-owned is subject to the user granting the school a right of inspection on request.

b. Requests for inspection can only be made in response to a specific cause for concern. Inspections will be carried-out by a member of the Headship team or escalated to a member of the Government of Jersey Police, should this be necessary. Devices will be ceased and turned off until such inspection. Staff would be encouraged to contact their Union should they have any concerns regarding this procedure.
c. Refusal to allow an inspection when one is requested will result in withdrawal of consent for the device to be used on-site (BYOD) or of immediate termination of the school-owned device. (see point 8) or if necessary, involvement of the Government of Jersey Police for further investigation.
d. School-owned devices must always be used in a manner that is consistent with the purposes for which they are provided: if inappropriate use is discovered during an inspection, then disciplinary action may be taken.

8. Withdrawal of Consent

I understand that…

a. Mobile devices can be used on-site, following acceptance of this agreement. Signed acceptance is not required: on-site use will be evidence of acceptance.
b. Contravening the terms of this agreement may result in withdrawal of consent to use BYOD or school-owned devices and, in extreme cases, disciplinary action and/or the involvement of third-party agencies, including MASH and/or Government of Jersey Police.
c. It is expected that staff using school-owned devices will bring those devices to school daily to support teaching and learning opportunities.
d. All school-owned devices are returnable immediately on demand.

Social Media (please refer to Social Media Policy)

I understand that…

a. Grouville uses www.grouville.sch.je and also Facebook to publish school information and to advertise and share school events.
b. Pictures taken on school property must not be added to **personal** social media without the permission of the Headship team. No photos of children, personal or sensitive data present in the background should be uploaded under any circumstances.
c. Staff will ensure professional boundaries exist between staff, parents and children by…
    - Not allowing a staff network login to be used by a child.
    - Only contacting parents through the agreed school systems and procedures.
    - Not becoming 'friends' with current children, or parents (unless already known on a personal capacity) on any social networking site.
d. Although social media is used as a personal forum, staff must be aware of protecting their professional identities through acting and posting responsibly online. (See Government of Jersey Social Media Policy)

School Actions & Sanctions

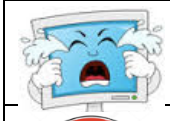
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in an appropriate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as outlined in the School Behaviour Policy. In the event of an illegal activity concern staff must follow the Child Protection & Safeguarding Policy Protocols as per policy.

Appendix 3

Grouville School
IT Responsible Use Agreement (RUA)
Younger Children EYFS / KS1

For your child to be able to use the technology at school they must follow these rules at all times. Following the rules below will allow your child to become a responsible, knowledgeable and safe user of technology.

Please read these expectations with your child carefully. Please complete the slip at the bottom of the page and return to the school office.

This is how we stay safe when we use technology	
	I will ask a teacher or suitable adult if I want to use school technology (computers, iPads or robotics).
	I will only access activities that a teacher or suitable adult has allowed me to use.
	I will take care of the computer and other equipment. I will hold iPads carefully and put them back correctly.
	I will ask my teacher for help if I am not sure what to do, or if I think I have done something wrong.
	I will tell my teacher if I see something that upsets me on the screen.
	I know not to talk to strangers online especially as some games and online services can have chat options.
	I will keep my personal information and passwords safe. I will always ask an adult if I am not sure.
	I will always be kind when using technology.
I know that if I break the rules I might not be allowed to use the school technology until I prove that I can be a responsible user.	

I have discussed the Responsible Use Agreement with my child. My child understands the rules and agrees to the follow them carefully.

Name of child: **Year Group:**

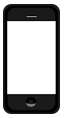
Parent/Carer signature: **Date:**

Appendix 4

Grouville School
IT Responsible Use Agreement (RUA)
Lower KS2 Responsible User Agreement

For your child to be able to use the technology at school they must follow these rules at all times. Following the rules below will allow your child to become a responsible, knowledgeable and safe user of technology.

Please read these expectations with your child carefully. Please complete the slip at the end of the RUA and return to the school office.

Lower Key Stage 2 Technology Rules	
	I will only use the internet when I have been given permission by my teacher. I will ask for help if I need guidance.
	I will keep my login details private. I will only use my own login details.
	I only email and message people that our teacher has approved. I will not reply to anyone who I do not know in person.
	I will think before I write. I will not post or send anything that is not appropriate, unkind or that could upset others. If I wouldn't want my teacher to see it-I won't type, click send, or post.
	I will never give out my personal information e.g. full name, address or phone number unless a responsible adult has instructed me to. I will not post information that could identify me in public such as videos in school uniform outside of school technologies.
	I will look after and respect our ICT equipment and resources in school. I will tell a teacher immediately if something does not work.
	If I see something that upsets me online, or feel that something is not appropriate, I will tell a teacher.
	I know that mobile phones and personal electronic devices cannot be used at school. I will turn them off and place them in the office mobile storage box until the end of the day.
	I know that my technology use is monitored and is not private. This information will be shared with my teacher and possibly my parents if I break the rules.
I know that if I break the rules, I might not be allowed to use the school technology until I prove that I can be a responsible user.	

Technology at Home: I will continue to use online services responsibly, safely and appropriately outside of school. I will report any concerns that arise from technology use at home to my parents, or if needed an adult who I trust at school. I will always check and follow the age rating guidance for apps and websites. I understand that it is my parent's/carer's responsibility to monitor my use of technology at home and will allow them to access my devices at home.

Grouville School
IT Responsible Use Agreement (RUA)
Lower KS2 Responsible User Agreement

To be able to use the technological facilities in our school you must agree and adhere to the rules outlined in the RUA at all times- this is to make sure you are safe. Following these rules will allow you to become a responsible, knowledgeable and safe user of technology.

Please keep the 1st page at home so you can reference this when necessary.

I have discussed the RUA with my child and my child agrees to the follow the rules that are outlined. Please sign and return to the office where this will be retained in your child's school file.

Name of child: ***Class:***

Parent's Signature: ***Date:***

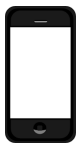
Child's Signature:

Appendix 5

Grouville School
IT Responsible Use Agreement (RUA)
Upper KS2 Responsible User Agreement

For your child to be able to use the technology at school they must follow these rules at all times. Following the rules below will allow your child to become a responsible, knowledgeable and safe user of technology.

Please read these expectations with your child carefully. Please complete the slip at the bottom of the page and return to the school office.

Upper Key Stage 2 Technology Rules	
	I will always use the internet responsibly. I will ask for help if I need guidance and access sites which are reputable.
	I will keep my login details private. I will only use my own login details.
	I only email and message people that our teacher has approved. I will not reply to anyone who I do not know in person.
	I will think before I write. I will not post or send anything that is not appropriate, unkind or that could upset others. If I wouldn't want my teacher to see it-I won't type, click send, or post.
	I will never give out my personal information e.g. full name, address or phone number unless a responsible adult has instructed me to. I will not post information that could identify me in public such as videos in school uniform outside of school technologies.
	I will look after and respect our ICT equipment and resources in school. I will tell a teacher immediately if something does not work.
	If I see something that upsets me online, or feel that something is not appropriate, I will tell a teacher. I will not view or share any material that is unsuitable. If I accidentally see any unsuitable material then I will turn off the screen and immediately tell a teacher.
	I know that mobile phones and personal electronic devices cannot be used at school-unless a teacher has made specific planned activity arrangements. I will turn devices off and place them in the office mobile storage box until the end of the day. They will stay turned off until I am off school premises.
	I know that my technology use is monitored and is not private. This information will be shared with my teacher and possibly my parents if I break the rules.
	I will only take photographs in school when I have permission to do so. I will not send or add any photographs taken on school property via messaging services or social media -Whatsapp, iMessage, Instagram, Tik Tok etc.
I know that if I break the rules I might not be allowed to use the school technology until I prove that I can be a responsible user.	

Technology at Home: I understand that it is my parent's/carer's responsibility to monitor my use of technology at home and will allow them to access my devices at home.

- I will continue to use online services responsibly, safely and appropriately outside of school. I will report any concerns that arise from technology use at home to my parents, or if needed an adult who I trust at school.
- I should make sure that my parents know what I am doing on my devices. I understand that my parents are responsible for my safety at home and this includes when I am using technology.
- I will use technology for a healthy amount of time and within the right environment – I will talk to my family about this and set a family agreement to ensure we all understand our family rules.
- I will always check and follow the age rating guidance for apps, services and websites. (Facebook, Instagram, Whatsapp & TikTok are for ages 13+ and are not suitable for primary aged students) however, if parents/carers choose to give permission for me to use these services they are aware of the risks and will carefully monitor my activity.
- I will never make 'friends' with anyone I do not know in real life.
- If I am in doubt about anything then I will ask my parents or a responsible adult for help or advice.

The most important part of this agreement is for you to know that you can always talk to your parents and teachers about anything that may worry you whilst using technology. Your safety is our upmost priority.

Grouville School
IT Responsible Use Agreement (RUA)
Upper KS2 Responsible User Agreement

To be able to use the technological facilities in our school you must agree and adhere to the rules outlined in the school section of our RUA at all times- this is to make sure you are safe. Following these rules will allow you to become a responsible, knowledgeable and safe user of technology.

Please keep the 1st page at home so you can reference this when necessary.

I have discussed the RUA with my child and they agree to the follow the rules that are outlined within it. Please sign and return to the office where this will be retained in your child's school file.

Name of child: ***Class:***

Parent's/Carer's Signature: ***Date:***

Child's Signature:

Appendix 6 ONLINE RISK ASSESSMENT TEMPLATE

Education Department Risk Assessment – DATA PROTECTION

Please complete a risk assessment for every third party web based service or application before you commence using that service. If your risk assessment demonstrates an unacceptable level of risk then do not use the service. Web based services are wide ranging and include any 'apps' (e.g. for iPad, Android), any cloud based service (e.g. Dropbox, iCloud) or any webmail provider (e.g Gmail, Hotmail, Yahoo Mail).

Personal data is defined as any data **identifying or relating to** a living individual. This includes photographs. *Note that an individual can be identifiable without being actually named* (e.g. year group and initials would likely be personal data), so be cautious. 'Sensitive data' will require an even higher level of caution. Each risk assessment should be reviewed annually.

This form should be completed either by the Headteacher or by the designated member of staff appointed by the Headteacher, before being copied to the Head of Governance at the Education Department. The Department will offer feedback and guidance on the risk assessment, but the ultimate decision as to whether the web based service should be used is for the data controller (school) to make.

Please complete this form while referring to the Data Protection (Jersey) Law 2005 available at jerseylaw.je

Note that any breach of data protection arising (whether from the use of a third party service or directly) should be reported to the Information Commissioner and the Head of Governance at the Educational Department.

Name of web based service or package/ third party provider			School name:		
Risk Assessment conducted by:		Date:		Date of review:	

The data being shared

Area of risk	Breakdown of risk. How probable is the risk? How severe would the repercussions be?	Analysis of these risks in the school context	How will these risks be mitigated? Can they? Who will be responsible?	Risk rating (low, medium, high)
Safeguarding. Risk of personal or sensitive personal data being shared to jurisdictions with no data protection legislation	Safeguarding – risk of actual harm/ emotional harm to individuals Risk of privacy breach to individuals Risk of prosecution by the Information Commissioner for			

	breaching the Data Protection Law Risk of complaints or litigation from parents or other individuals – financial Reputational risk (note that the reputational and safeguarding risk is higher in Jersey due to children being more easily identified) Define who will be using the service- named members of staff? If the service is to be used directly by pupils consider how you will manage the increased risk Any other safeguarding risks			

Area of risk	Breakdown of risk. How probable is the risk? How severe would the repercussions be?	Analysis of these risks in the school context	How will these risks be mitigated? Can they? Who will be responsible?	Risk rating (low, medium, high)
Risk of sensitive data being processed in breach of the Law *Sensitive data includes:*	*N.B Sensitive personal data cannot be processed unless one of the following conditions is met:* ● Explicit informed consent ● Employment obligations			

the racial or ethnic origin of Data Subject; political opinions; religious or other beliefs of a similar nature; membership of trade unions; physical or mental health or condition; sexual life; the commission of any offence or criminal records	• Vital interests of data subject *or another person* • Non-profit organisations – political, philosophical, religious, trade unions • Information already been made public by data subject - deliberately • Legal proceedings/advice • Public functions • Medical purposes – health professional – preventative medicine • Equal opportunity research			

Area of risk	**Breakdown of risk. How probable is the risk? How severe would the repercussions be?**	**Analysis of these risks in the school context**	**How will these risks be mitigated? Can they? Who will be responsible?**	**Risk rating (low, medium, high)**
Personnel and communication risk. Web based service or third party provider being signed up to by staff or students without an awareness or assessment of the risks or going through the data protection	The responsibility and liability would likely still ultimately lie with the school as data controller, regardless of whether the staff member signed up on their own volition. Consider how to ensure communication of the risk and how you would ensure that all		•	

officer or due process	services are signed up to only through the data protection officer Consider training			
Data security issues	• Devices holding personal data or with access to web based services leaving the premises • Encryption not being used • Weak or inadequate passwords		•	

Is the use of this service or third party viable, taking into consideration the above risks?
If so, who will be responsible for monitoring the risks and terms and conditions?
Next review date for this risk assessment (recommended annually)
Has the use of this service been included on the school's fair processing statement and the change communicated to parents?
How will you communicate the above to members of staff?
Signed: Print name and position: