Grouville School Digital Safeguarding Policy 2017

UNRC Article 3: Everyone who works with children should do what is best for each child.
UNRC Article 19: Children should not be harmed and should be looked after and kept safe.
UNRC Article 36: Children should be protected from doing things that could harm them.

This document is written based around the Education Department's 'Digital Safeguarding (E-Safety) Policy' and is written for the context of Grouville School. It covers all aspects of online and offline activities and behaviour, including the use of devices that are both school owned and student/staff owned.

The policy's primary intention is to safeguard students and members of staff at Grouville School and to ensure they maintain their own digital safeguarding beyond the school gates. Grouville School has a duty of care under the Law to assess and prevent possible harm to children. The field of digital safeguarding, also known as E-safety, is constantly evolving with the pace of technological change and schools need to manage the attendant risks actively and in a timely manner in order to achieve effective digital safeguarding.

The change in terminology from E-safety to digital safeguarding indicates a change in emphasis; away from the former's association with pure technology towards the latter's alignment with other areas of safe practice. Many of the issues that arise in digital safeguarding are behavioural and their management is no different from ensuring appropriate behaviour in any other area of school life or professional activity. Digital safeguarding should therefore be addressed with due regard to other applicable policies including; Child Protection, Anti-Bullying, Health and Safety, Data Protection and Uses of Photographs of Children as well as applicable laws such as Freedom of Information.

Key Roles and Responsibilities

The Education Department will:

- Maintain a Digital Safeguarding Officer with overall responsibility for this area within the department to offer schools and the Department expert advice, guidance and recommendations. He/she will also create and update supporting documentation and resources and arrange central training.
- Monitor and review schools' safeguarding delivery through its Digital Safeguarding Officer.
- Provide supported networks for hard-wired and, where applicable, mobile devices.
- Provide technical assistance for the systems that it supports via the IT helpdesk.
- Create mechanisms whereby schools that wish to do so may take greater control over the deployment and use of digital safeguarding solutions.
- Continue to offer managed solutions for digital safeguarding to those schools that are not yet ready to manage their own deployment.

Grouville School will:

- Identify at least one Digital Safeguarding Officer to monitor, review and develop best practice: the Coordinator will also be the primary contact between the school and the Department in all matters of Digital Safeguarding. Currently this is Jo Nayar.
- Ensure that the identified individual is given sufficient time to complete this role and that the identified individual is trained to a high level, equivalent to CEOP (Child Exploitation and Online Protection) Ambassador.
- Ensure digital safeguarding is given a suitably high priority and in the school's development and improvement planning. Digital safeguarding logs, risk assessments and other documents must be available to the Department on request.
- Ensure all members of staff are appropriately trained in digital safeguarding by the schools Digital Safeguarding Officer or Coordinator who may draw on Department resources to complement the school's own in house expertise.
- Always safeguard the digital wellbeing of members of staff by, for example, not publishing any of their personal details (including photos) online without consent. Schools must not require staff to use personal mobile phones to communicate with parents or students at any time: schools must provide school-owned devices that can be used whenever mobile communication is needed.
- Evaluate and risk assess new technologies to ensure that the anticipated educational benefits justify any potential digital safeguarding risks that might be identified, including likely misuse of the technologies.
- Ensure that an outline of the school's approach to digital safeguarding, including responsible use of technologies and appropriate technology based behaviour is communicated to all stakeholders.
- Ensure that all children are aware of their responsibilities and regularly updated about digital issues in a meaningful and engaging manner.
- Ensure that parents and carers are aware of their responsibilities and regularly updated about digital safeguarding issues at an appropriate level in newsletters and that appropriate content is found on the school website for parents to access.

School Digital Safeguarding Coordinators 's Key Responsibilities

Training and Support

- Have a clear understanding of child protection, digital safeguarding and data protection policies and be able to determine the applicable policies for different situations.
- Have undergone appropriate training, such as CEOP Ambassador, to acquire a detailed insight into current concerns and consequences of particular situations and actions. Incidents of sexting, for example, must be reported to the school's Child Protection Officer and referred to the MASH team.
- Have a solid pedagogical insight that can assess the learning benefits of any change when balanced with the associated potential digital safeguarding risks.

- Attend relevant update training and support sessions, both on-island and elsewhere to remain aware of the latest concerns and best practices.
- Ensure members of staff are informed about lines of external support that are available, such as the Professionals' Online Safety Helpline (helpline@saferinternet.org.uk) operated by the UK Safer Internet Centre.
- Challenge and support members of staff to develop their awareness of and teaching about digital safeguarding.

Monitoring Practice

- Develop and keep up-to-date the Digital Safeguarding Policy which must accurately reflect the requirements of the Department's Digital Safeguarding Policy and the school's own practice.
- Develop appropriate and differentiated Responsible Use Agreements (RUAs) and ensure these are signed by staff, children and parents. Ensure that signed RUAs are filed for future reference if required. Ensure there are clearly understood measures to deter and reform inappropriate behaviour.
- Establish, monitor and maintain a Digital Safeguarding Log in which are recorded all issues as they arise, together with a Digital Safeguarding Risk Assessment File detailing concerns and potential new development to show that risks have been appropriately considered and are periodically reviewed.
- Audit practice across the school and produce an action plan to improve the schools digital safeguarding provision using a self-evaluation framework such as SWGFL's 360 Safe (www.360safe.org.uk).
- Ensure that public communications through digital channels, including social media, are appropriately managed and consistent with all applicable policies.
- Brief staff regularly on digital safeguarding developments.
- Ensure that our digital safeguarding programme is taking place by monitoring weekly planning and ensuring there are one Key Stage 1 and 2 assemblies per term on E-Safety issues.

Managing Systems

- Monitor that these are put in place to reduce and, where possible prevent inappropriate behaviour and the accessing of unacceptable content.
- Manage and maintain different user profiles for web filtering to provide protection as appropriate and flexibly as required.
- Conduct active testing to ensure that blocked content remains inaccessible.
- Monitor the selection of all web based service by members of staff to ensure use is consistent with the Term and conditions (including minimum age) and with all legal requirements (including Jersey Data Protection Law).

- Encourage appropriate use of file storage locations and of encrypted memory sticks for the transportation of personal data.
- Ensure procedures are in place to prevent digital safeguarding decisions being taken by technical staff.
- Convey clear messages and employ workable measures to discourage users from connection to external networks whilst on school premises.
- Monitor the schools online profile and presence, including unofficial sites.

Staff Members' Key Responsibilities

- Act on all digital safeguarding issues promptly and in accordance with the school's Digital Safeguarding Policy
- Be diligent when digital safeguarding issues suggest child protection concern: follow child protection procedures immediately in these circumstances.
- Work within the schools digital safeguarding measures and not attempt to compromise or circumvent those measures.
- Protect professional boundaries by, for example, not giving students a member of staff's mobile number, not allowing a staff network log-in to be used by a student and not becoming friends with students on social media sites.
- Be diligent in respect of data protection: use encrypted memory sticks whenever possible and ensure that data is always kept in authorised jurisdictions.
- Select websites for school use only after reviewing Terms and Conditions, especially in regard to data protection compliance and minimum permitted age.
- Seek advice from the school's Digital Safeguarding Coordinator whenever necessary to discuss concerns, develop best practice and support students.
- Sign an RUA and be aware of the responsibilities bestowed by that Agreement.

Pupil's' Key Responsibilities

- Work within the school's digital safeguarding measures and try not to compromise or bypass these measures.
- Know how and whom to report anything to that could improve the digital safeguarding environment and the digital/online wellbeing of students.
- Respect personal privacy and keep their own personal information private, including photographs and passwords.
- Be aware of and contribute towards any support systems that encourage students to discuss digital safeguarding concerns they may have, including peer to peer support and opportunities to talk to members of staff.

- Behave in a healthy and positive manner towards digital technologies when engaging in online activities.
- Read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of web services, especially with regard with the minimum age that some companies set for their websites in order to protect young people from risk .
- Sign an appropriate RUA and understand what that agreement means.

Parents' Key Responsibilities

- Discuss the school's RUA with their child(ren) and explain its implications at school and at home.
- Access support systems in school and via the Internet to develop appropriate awareness of how to protect their child.
- Talk through concerns about digital safeguarding with an appropriate member of staff as necessary.
- Know how and who to report concerns to in order to improve the digital safeguarding environment and protect their child both at home and at school.
- Work with the digital safeguarding measures the school has in place.
- Respect digital safeguarding and data protection advice when sharing images, videos and text, especially personal information on social networking sites.
- Respect school passwords and encourage their child never to attempt to obtain or use another child's or adult's password.
- Encourage their child to read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of web services, especially with regard with the minimum age that some companies set for their websites in order to protect young people from risk.

Monitoring and Review

The Leadership Team monitors any Digital Safeguarding Concerns in order to ensure that all issues are handled properly.

Other documents to refer to

RUA (for children, parents and staff)
Computing Curriculum Policy
Parent Social Media Policy
July 2016 Online Safety – Policies and Procedures for the Education Dept and Youth Service

Adapted by Jo Nayar April 2017
To be reviewed April 2019