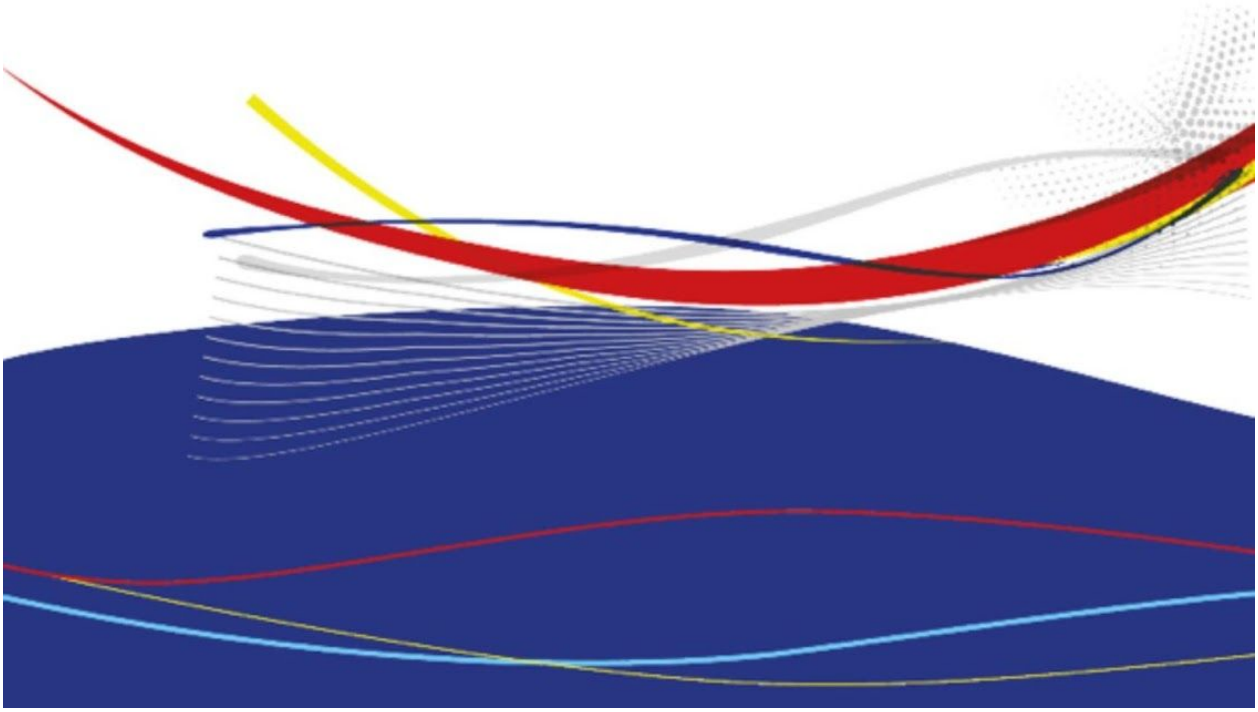
Les Quennevais School

Digital Safeguarding Policy

Updated May 2015



Development / Monitoring / Review of this Policy

This digital safeguarding policy has been developed by the Digital Safeguarding Coordinator with input from:

DfESC, Deputy Head Teacher, Data Protection Officer

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Information provided by DfESC who manage the filter
- Surveys / questionnaires of students, parents / carers and staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of the school. The terms e-safety and digital safeguarding are interchangeable for the purposes of this policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour.

Contents

Roles and Responsibilities

The following section outlines the digital safeguarding roles and responsibilities of individuals and groups within the school.

Head Teacher & SLT

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Digital Safeguarding Coordinator.
- The Head teacher and Deputy Head with responsibility for Safeguarding should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flowchart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant DfESC disciplinary procedures.
- The Head teacher and Deputy Head with responsibility for Safeguarding are responsible for ensuring that the Digital Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Digital Safety Coordinator

Digital Safeguarding Coordinator:

- takes day to day responsibility for digital safeguarding issues and has a leading role in establishing and reviewing the school digital safeguarding policy
- ensures that all staff are aware of the procedures that need to be followed in the event of digital safeguarding incident taking place.
- provides training and advice for staff
- liaises with DfESC
- liaises with school technical staff
- receives reports of digital safeguarding incidents and creates a log of incidents to inform future digital safeguarding developments.
- reports to Senior Leadership Team

Network Manager:

Overall network security and internet filtering is currently controlled externally by DfESC. The Network Manager should assist DfESC in ensuring:

- that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required digital safeguarding technical requirements and follows DfESC guidelines
- that users may only access the networks and devices through a properly enforced password protection policy.
- that they keep up to date with digital safeguarding technical information in order to effectively carry out their digital safeguarding role and to inform and update others as relevant
- any misuse / attempted misuse can be reported to the Digital Safeguarding Coordinator and/or SLT for investigation / action / sanction

Teaching and Support Staff:

are responsible for ensuring that:

- they have an up to date awareness of digital safeguarding matters and of the current digital safeguarding policy and practices
- they report any suspected misuse or problem to the Digital Safeguarding Coordinator for investigation.

- all digital communications with students/ parents / carers should be on a professional level and only carried out using official school systems
- digital safeguarding issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the digital safeguarding and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Safeguarding Officer:

should be trained in digital safeguarding issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good digital safeguarding practice when using digital technologies out of school and realise that the school's digital safeguarding Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these. Parents and carers will be encouraged to support the school in promoting good digital safeguarding practice and to follow the guidelines contained within this document on the appropriate use of:

- digital and video images taken at school events
- their children's school Account
- their children's personal devices in the school

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in digital safeguarding is therefore an essential part of the school's digital safeguarding provision. Children and young people need the help and support of the school to recognise and avoid digital safeguarding risks and build their resilience.

Digital Safeguarding should be a focus in all areas of the curriculum and staff should reinforce digital safeguarding messages across the curriculum. The Digital Safeguarding curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned digital safeguarding curriculum should be provided as part of ICT and PSE lessons and should be regularly revisited
- Key digital safeguarding messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Education – parents / carers

Many parents and carers have only a limited understanding of digital safeguarding risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

It is essential that all staff receive digital safeguarding training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of digital safeguarding training will be made available to staff. This will be regularly updated and reinforced. An audit of the digital safeguarding training needs of all staff will be carried out regularly.
- All new staff should receive digital safeguarding training as part of their induction programme, ensuring that they fully understand the school digital safeguarding policy and Acceptable Use Agreements.
- The Digital Safeguarding Coordinator will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

Currently the network infrastructure and filtering is managed externally by the DfESC. The school will assist them in ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their digital safeguarding responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager should also be available to the Head teacher and kept in the school safe
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. School / a technical staff and teachers monitor and can record the activity of users on the school technical systems (e.g. Imperio) and users are made aware of this in the Acceptable Use Agreement
- All users will be provided with a username and secure password by the Network Manager. Users are responsible for the security of their username and password

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. The school has a BYOD policy in place and this can be found in the appendices to this policy.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Jersey Data Protection Law principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated where appropriate
- Where possible these devices will be covered by the school’s normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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.

- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Jersey Data Protection Law). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere (including on official school social media sites such as facebook and twitter) that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Jersey Data Protection Law (2005) 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.

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained and lawfully processed.
- It is registered as a Data Controller
- Responsible persons are identified and risk assessments are carried out by the Data Protection Officer
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- Any use of cloud storage must be authorised and follow the DfESC guidelines on web based applications and the school's own guidelines (see appendices).

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

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

- The official school email service may be regarded as safe but must not be used to transfer any sensitive data. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the Digital Safeguarding Coordinator or Senior Teacher with responsibility for safeguarding, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use, social media risks, checking of settings, data protection, reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character)					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)			X			
Online gaming (non educational)					X	
Online gambling					X	
Online shopping / commerce				X		
File sharing				X		
Use of social media			X			
Use of messaging apps			X			

Use of video broadcasting eg Youtube		X			

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer immediately to the Deputy Head Teacher with responsibility for safeguarding. Information on the subsequent procedure can be found in the appendix (responding to incidents of misuse)

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. These incidents should be reported to SLT/Digital Safeguarding Coordinator/Network Manager as appropriate. Further information can be found in the appendix (responding to incidents of misuse/other incidents).

School / Academy Actions & Sanctions

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

The following list of actions would lead to sanctions being taken. The sanctions would vary according to the severity of the incident could include warnings, detentions, referral to Head of Department/Year/Head teacher/Police.

Students / Pupils

Incidents:
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
Unauthorised use of non-educational sites during lessons
Unauthorised use of mobile phone / digital camera / other mobile device
Unauthorised use of social media / messaging apps / personal email
Unauthorised downloading or uploading of files
Allowing others to access school / academy network by sharing username and passwords
Attempting to access or accessing the school / academy network, using another student's / pupil's account
Attempting to access or accessing the school / academy network, using the account of a member of staff
Corrupting or destroying the data of other users
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
Continued infringements of the above, following previous warnings or sanctions
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
Using proxy sites or other means to subvert the school's / academy's filtering system
Accidentally accessing offensive or pornographic material and failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Receipt or transmission of material that infringes the copyright of another person or infringes the Jersey Data Protection Law

For Staff the following list gives examples of actions that may lead to disciplinary action and/or police involvement

Staff

Incidents:
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
Inappropriate personal use of the internet / social media / personal email
Unauthorised downloading or uploading of files
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
Careless use of personal data eg holding or transferring data in an insecure manner
Deliberate actions to breach data protection or network security rules
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils
Actions which could compromise the staff member's professional standing
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy
Using proxy sites or other means to subvert the school's filtering system
Accidentally accessing offensive or pornographic material and failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Breaching copyright or licensing regulations
Continued infringements of the above, following previous warnings or sanctions