Janvrin School

Digital Safeguarding Policy

Preamble:
Access and use of digital technologies are now an integral part of most people's lives and, for our current generation of children, a resource which has always been a part of their lives.
The speed with which technologies and devices develops is staggering and poses potential risks for our ability to truly understand the capacity of APPs, programmes, devices and social media etc.

The internet and other digital and information technologies are powerful tools, which can help teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Children and young people should have an entitlement to safe internet access at all times. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate all those risks completely. It is therefore essential, that the school educates, nurtures and guides children in to lifelong safe and appropriate habits of access to the internet and other digital sources of information and communication.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The digital safeguarding policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy
This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors) who have access to and are users of school ICT systems, both in and out of school.

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 digital safeguarding behaviour that take place out of school.

Roles and Responsibilities

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

Headteacher and Senior Leaders

The Headteacher is responsible for ensuring the safety (including digital safeguarding) of members of the school community,

The Headteacher / Senior Leaders are responsible for ensuring that the Digital Safeguarding Officer and other relevant staff receive suitable CPD to enable them to carry out their digital safeguarding roles and to train other colleagues, as relevant.

The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious digital safeguarding allegation being made against a member of staff.

Digital Safeguarding Officers (Headteacher, Assistant Headteachers and Computing Lead)

- take day to day responsibility for digital safeguarding issues and have a leading role in establishing and reviewing the school digital safeguarding policies / documents;
- ensure that all staff are aware of the procedures that need to be followed in the event of a digital safeguarding incident taking place;
- provide digital safeguarding training and advice to staff in accordance with Department for Children, Young People, Education and Skills (CYPES) guidelines;
- liaise with and attend meetings with the Department for CYPES Digital Safeguarding Officer
- liaise with the school ICT technician;
- receive reports of digital safeguarding incidents (IMPERO and Lightspeed) and respond in an appropriate and consistent manner in line with Department for CYPES policies and procedures.
- create and maintain a log of incidents to inform future digital safeguarding developments;
- report regularly to Senior Leadership Team to discuss current issues and review incident logs.
- liaise with the Department for CYPES Digital Safeguarding Officer to disseminate digital safeguarding information to parents and the wider community.

Network Manager / Technical staff

The Computing Lead and ICT Technician are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the digital safeguarding technical requirements outlined in the Department for CYPES **Digital Safeguarding Policy** and guidance and **Responsible Use Policy**
- that users may only access the school's networks 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
- that the use of the network / website/ email is regularly monitored in order that any misuse / attempted misuse can be reported to the Digital Safeguarding Officer /Headteacher / for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies;

- that risk assessments are carried out and reviewed for any computing, including web-based risk assessments.

Teaching and Support Staff
The Teachers and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of digital safeguarding matters and of the current school digital safeguarding policy and practices.
- they have read, understood and signed the school Staff Responsible Use Policy / Agreement (RUP)
- they report any suspected misuse or problem to the Digital Safeguarding Officer /Headteacher for investigation.
- digital communications with students / pupils (email) / Google Classroom / Office365/social media/InTouch/ voice) 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 school activities • pupils understand and follow the school digital safeguarding and Responsible use policy.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor ICT activity in lessons, extra-curricular and extended school activities.
- they are aware of digital safeguarding issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- in lessons where internet use is pre-planned students / pupils 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
- Digital safeguarding is a focus in all areas of the curriculum and staff reinforce digital safeguarding messages in the use of ICT across the curriculum.

Designated Safeguarding Lead/Child Protection
The DSL should be trained in digital safeguarding issues and be aware of the potential for serious child protection 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

Pupils

- are responsible for using the school ICT systems in accordance with the Pupil Responsible Use Policy which they will be expected to sign before being given access to school systems.
- 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 school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school 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.
Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national / local digital safeguarding campaigns / literature.

Digital safeguarding education will be provided in the following ways:

- An integrated digital safeguarding programme will be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key digital safeguarding messages should be reinforced as part of a planned programme of assemblies and PSHE activities;
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Pupils should be helped to understand the need for the student / pupil RUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Pupils 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 ICT, the internet and mobile devices

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

- Letters, newsletters, InTouch, website, social media
- Parents evenings
- Reference to appropriate websites
- Highlighting concerns about inappropriate web-sites from CYPES, the Police, parents and wider school community

Education & Training – Staff
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:

- All new staff should receive digital safeguarding awareness raising as part of their induction programme, ensuring that they fully understand the school digital safeguarding policy and Responsible Use Policies
- The Digital Safeguarding Officer will receive regular updates through attendance at CYPES training sessions and by reviewing guidance documents from CYPES;
- This Digital Safeguarding policy and its updates will be presented to and discussed by staff in staff meetings.

Technical – infrastructure / equipment, filtering and monitoring
In line with CYPES policy, the school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the digital safeguarding technical requirements outlined in the CYPES Online Safety Policy
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by the ICT Technician who will keep an up-to-date record of users and their usernames.

- The ICT Lead/Digital Safeguarding Team and a nominated Senior Leader should have "administrator" rights for the school ICT system,
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Department for CYPES
- Any filtering issues should be reported immediately to Department for CYPES
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and ICT Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly;
- Department for CYPES ICT technical staff regularly monitor and record the activity of users on school ICT systems and users are made aware of this in the Responsible Use Policy.
- Remote management tools are used by staff at Department for CYPES/C5 to control workstations and view users activity;
- An appropriate system (My Concern) is in place for users to report any actual / potential digital safeguarding incident to the Digital Safeguarding Officer
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- "Guests", such as supply teachers, visitors will be allowed access to the school network by means of a Guest user name and password. "Guests" with free access will be required to sign a Responsible Use Policy.
- It is agreed that any documents/devices with specific information on are password protected this applies to the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- The school infrastructure and individual workstations are protected by up-to-date virus software.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

There are many reported incidents of employers carrying 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 / pupils 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.
- Staff 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 be avoided for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are only participating in appropriate activities.

- Students / pupils must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written consent from parents or carers is obtained on the school information sheet, allowing for images to be published;
- Pupil's work will only be published with the permission of the pupil and parents or carers.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils 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 need to be aware that email communications may be monitored;
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Should such an incident occur, it should be reported immediately to the Digital Safeguarding Officer who will refer to the Department for CYPES document "Online Safety Policy" and decide upon an appropriate course of action.