Bel Royal School Online Safety Policy

Version: 1.0	Valid from: February 2022	Author: J Baudains, K Simon
Version 1.1	Valid From November 2022	Updated by C .Hammond
Version 1.2	Valid form February 2024	Updated by C .Hammond

Aims and Purpose

The purpose of the online safety policy is to highlight our schools' safeguarding obligations in keeping young people safe online in a technologically developing world.

This policy applies to all school staff, including volunteers, whether they are accessing the school IT services within or outside of the school building.

The policy aims to make it clear the expectations on all school leaders, teaching and support staff, volunteers, parents, pupils and visitors. The policy also makes clear the procedures that are in place and will be followed to monitor and respond to online safety issues.

Online safety is not purely about technology. Many of the issues arising in online safety are behavioural and will be managed in the same way as in any other area of school life. Therefore, this policy should be read in conjunction with the Child Protection Policy and other safeguarding policies:

- Safeguarding and Child Protection Policy
- Behaviour Policy (inc. Counter Bullying Policy)
- Staff Handbook

Principles

Bel Royal School is a Rights Respecting School, and we teach our children about the articles of the UNCRC. Within this, these articles form the main principles of this policy:

- **Article 3 (best interests of the child)**: The best interests of the child must be a top priority in all decisions and actions that affect children.
- **Article 16 (right to privacy):** Every child has the right to privacy. The law should protect the child's private, family and home life, including protecting children from unlawful attacks that harm their reputation.
- **Article 19 (protection from violence, abuse and neglect):** Governments must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and bad treatment by their parents or anyone else who looks after them.
- **Article 34 (sexual exploitation)**: Governments must protect children from all forms of sexual abuse and exploitation

All children and staff have the right to be safe online, learn how to stay safe and the opportunity to explore the benefits of living in a technologically connected world. Within school we have tight monitoring and filtering systems, but we realise that it is less likely thee exist in pupil's homes or on their mobile devices.

Traditional Online Safety messages such as 'don't post personal information online' are less significant in today's world where social media is prevalent and is built on sharing personal information. Instead, we promote a more realistic and pragmatic approach whereby we encourage a culture where children and young people feel able to share concerns with a trusted adult and discuss online safety issues openly.

We encourage them to consider the scope of the potential audience to whom they are posting, the context they are posting in and to take responsibility for any potential consequences. They should understand that nothing put online can ever truly be considered 'private.'

However, the school will deal speedily and robustly with online safety incidents within this policy (and associated behaviour and anti-bullying policies) and will as relevantly inform parents / carers of incidents of inappropriate Online Safety behaviour that take place in or out of school. Any escalation or response will reflect the approaches taken with any other safeguarding escalation procedures or behavioural responses.

Online Risks

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

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

Learning to recognise warning signs will allow trusted adults to intervene where appropriate and to lessen the impact of potential negative experiences.

Roles and Responsibilities

School Responsibilities:

- Oversee and monitor the safe use of technology when children are in our care and act immediately if they are concerned about wellbeing (Lightspeed Systems, Impero.
- Ensure that all staff receive appropriate online safety training that is relevant and regularly updated;
- Ensure there are processes and mechanisms in place to support young people and staff facing online safety issues and these are publicised and transparent for young people to follow;
- Implement online safety policies and acceptable use policies, which are clear, understood and respected by all;
- Educate young people, parents and the school community to build knowledge, skills and capability in online safety;
- Monitor how the school is portrayed online by parents, children and staff;
- Not request a website/ digital application or software to be unblocked or installed unless a risk assessment has been completed;

Staff Responsibilities: Staff must:

- Ensure pupils understand and follow the online safety and acceptable use policies
- Act on and escalate all online safety issues promptly and escalate to the designated online safety individual in the school in accordance with the Child Protection and other Safeguarding policies;
- Sign a responsible use agreement and adhere to the responsibilities set out therein;
- Ensuring that they are properly "logged-off" at the end of any session in which they are using personal data and lock their machine when they leave the room (Ctrl/Alt/Del).

- Only use work email address to communicate with other staff, parents and children (not personal email); Personal email addresses, text messaging or social media must not be used for these communications.
- Ensure any digital communication between staff and students / pupils or parents / carers (email) is professional in tone and content.
- If working remotely from home: do not divulge the password to any family members or let any member of the household use the login, laptop or device for any purpose whatsoever; use a designated room or space to work from; keep the device always locked up and secure;
- Use every appropriate opportunity to link online safety into the everyday curriculum;
- Encrypt personal data (especially if transferring information, this should be via encrypted USB or encrypting software);
- Only use websites and web-based applications with students when they have been risk assessed and you have read and reviewed the terms and conditions and are satisfied that they do not pose a significant online safety or data protection risk;
- Not allow anyone else (whether children or other members of staff) to use their log on details or leave their computer or device unattended when logged into;
- Not send friend requests to or accept friend requests from students (even after they have left school, until they are 18) or parents on social media platforms. It is acknowledged that sometimes this is complicated due to relatives etc. however caution should always be exercised in respecting professional boundaries;
- Not attempt to compromise or bypass online safety measures for the sake of expedience or convenience.
- Ensure they have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices
- Monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed)
- Ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- In lessons where internet use is pre-planned 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
- Not connect any school device to an unsecured wifi network or 3G/4G network as this will bypass safeguarding filters.

<u>Designated Online Safety Lead:</u> Responsible for:

- Ensuring that children are educated about online safety and related issues;
- Monitoring online activity of children;
- Escalating safeguarding concerns where appropriate if there are safeguarding concerns, within the school and to the CYPES Department and other agencies such as MASH where appropriate;
- Maintain a log of online safety incidents in the school along with any follow up;
- Be responsible for approving and risk assessing the use of any web-based applications that staff wish to use;
- Reviewing school online safety and practice.
- Establish and review the school Online Safety policies / documents
- Ensure all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provide training and advice for staff.
- Ensure only authorised users may access the networks and devices and that they sign an AUP.
- Planning and monitoring the Online Safety curriculum and assembly provision.

- Attending update training and by reviewing guidance documents released by relevant organisations.
- Monitor the selection of web-based services staff are using, and where relevant, check they are risk assessed.
- Monitor the school's online profiles and reputation, including on unofficial sites.
- Conduct regular testing to ensure blocked content is still inaccessible

Pupils:
We ensure that all children in their care are aware of their responsibilities around appropriate use of technology both inside and outside of school. This awareness is delivered in lessons (PSHE and IT primarily), assemblies, events, newsletters and through the development of a culture of online safeguarding.

Pupils:
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 online safety practice when using digital technologies out of school and realise that the school's Online Safety 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 pro-actively engage parents and carers about online safety and related issues through newsletters, weblinks and events in school. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
- digital and video images taken at school events
- access to parents' sections of the website / blog
- their children's personal devices in the school (where this is allowed)

Parents are expected not to share offensive/disparaging comments about the school, members of staff or pupils on social media, and instead talk to the school about any concerns they have directly, so these can be actioned and resolved. Online comments from parents that are inappropriate will be followed up and possibly referred to the Police.

We recommend parents use websites such as www.commonsensemedia.org to help them to check apps before allowing their child to access no matter what their child says about 'everyone else has it'! This will help the parents make an informed view about what they deem to be safe or not.

Internet Filtering and Monitoring:
Our internet content is filtered centrally by the CYPES Department. This will remove most of the undesirable content, but it is important to bear in mind that no filtering system is infallible, and some unpleasant content will inevitably sometimes get through. This is particularly true of image searches, where some unpleasant images are tagged with innocuous words. Therefore, staff ensure there is sufficient supervision in place, and we encourage children to report concerns immediately to a member of staff.

In addition, CYPES monitors Google searches made on the school network. Any suspicious searches are flagged, and a report is automatically sent to the school designated leads for online safety each day. These reports are monitored daily, and action taken as required.

In concerns are raised, the staff member will liaise with the Online Safety Lead to make a judgement in context about any suspicious search activity and the appropriate action to take. This will consider the age of the child, the context of the issue and whether there have been any previous incidents. If there are ongoing safeguarding and welfare concerns, then any observations of online activity should be documented and integrated into this.

It would be usual practice for incidents to be followed up in line with the school's behaviour policy and where appropriate for parents to be informed. This may be led by the Online Safety Lead, or by the class teacher depending on the severity of the incident. In more serious or repeated cases the sanction may be to temporarily suspend the user's account and so access to computers and the internet. In most cases, a discussion about the issues, education, and clarification of the expectations will be sufficient to prevent further issues.

Deciding which apps, programmes and websites to use in lessons
Many digital 'apps' can circumvent the central monitoring and filtering and vigilant monitoring of this needs to be undertaken. Apps will only be installed once they have been risk assessed.

Websites and programmes need to be checked in advance, including viewing prior to the lesson Youtube and other media content as this can be changed to contain concerning content if viewed 'live.

Web Histories
For safeguarding reasons, it may occasionally be deemed necessary to look at the web history of a child. The search and the reasons for the report should be documented in the child's file, and the outcome of the report integrated within any other child protection procedures.

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

Mobile devices
Mobile devices accessing the internet via the 3G or 4G networks are not subject to the same filtering and monitoring that the school systems are. We do not allow children to use 3G/4G technology or their own phones/tablets in school, including smart watches.

Children may bring their phones to school, but these must be kept turned off and out of sight until the end of the school day and only used once the when the child has left the school grounds. Smart watches may not be brought to school.

Staff may not use their personal mobile devices for work purposes, such as to take photos etc. Staff have access to Ipads and digital cameras for photographs, and there is a school phone that must be used on school trips etc.

Social Media
Social media is recognised as a particular risk area for children. The school does not promote the use of social media nor use it in learning. Although we teach children about

the risks involved, we do not teach children directly how to use these sites. Most social media sites have an age restriction of 13, and therefore none of the children in our school should be accessing social media or have their own site.

Staff do use Youtube and other media hosting sites to share educational videos and content during lessons, however, this content is always checked, and ideally downloaded, first.

All staff should ensure that their personal Social media profiles are locked down and not publicly viewable, bearing in mind that default privacy settings change regularly and that there is really no such thing as 'private post' on social media.

If parents or members of the community post negative comments about the school or staff students in the school, staff should escalate this to the Headteacher who should seek advice from the Head of Governance at the Department.

Online Bullying
(Please read in conjunction with our Safeguarding and Counter Bullying Policies).

Bullying can happen both on and offline. While online bullying can be an extension of face-to-face bullying, it differs in several significant ways:

- the invasion of home and personal space;
- the difficulty in controlling the scale and scope electronically circulated messages;
- the size of the audience;
- perceived anonymity;
- the profile of the person doing the bullying and their target is often different.

The school will respond to online bullying in accordance with our Counter Bullying Policy. Online bullying like any other kind of bullying will not be tolerated in the school.

Children that believe they have been bullied online should report this to parents, a trusted member of staff or online, through the many reporting functions. Children will be treated with respect and sympathy if they disclose bullying. Existing pastoral support procedures will be used to support the child. Allegations of bullying will be rigorously followed up and swift action taken. Actions will be recorded on our log and also on the child's file.

Where there is an allegation of bullying online, the child should keep the evidence and take it to their parent or a member of staff.

Self-harm
A Journal of Adolescence report, 2017 suggests the role of the Internet has a significant factor in young people self-harming. Self-harming can start with children as young as ten. Children that self-harm may use the internet for research into self-harming practices, exploring online imagery and research social media platforms where this is being discussed. If our monitoring software flags up a term relating to self-harm, this will be responded to as a matter of urgency, in line with Child Protection procedures.

Radicalisation
Paragraph 7 of the Prevent Duty (UK Government advice for schools) defines extremism as: 'vocal opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces.' As a school we have a duty to try to prevent people from being drawn into terrorism. This duty includes monitoring for signs of radicalisation. As extremist groups aim to target young

people who are perhaps lonely, disenfranchised and want to feel part of a community. This can happen to any child of any background, in any geographical location who is using the internet, and Jersey is not immune.

Sexting

Sexting is a term which describes the sharing of intimate images with others, using online technologies. Sexting is an increasing phenomenon among children, even of primary age. Creating or sending an intimate photo of a minor (if reported as a complaint by the police) is technically a criminal offence, so incidents need very careful management. If staff become aware of sexting using a device, they will secure the device and switch it off, and seek advice from the Designated Safeguarding Lead who will follow normal child protection procedures.

18 rated games and films

There is a growing phenomenon of children playing adult rated first-person games such as Call of Duty or Grand Theft Auto. These games contain extreme violence, sexually explicit content, images of drug taking and other adult themes. In addition, children have access to adults from all over the world via the headset and multi-player options, which creates an added risk. Research shows that parents often buy these games for their children, so working in partnership with parents and carers is crucial in tackling this issue. Where staff become aware of children playing games such as these, it is possible child protection procedures will be followed depending on the individual context.

Online Activity Concerns

A child's behaviour online does not exist in a vacuum. It is often an extension of their situation offline. Therefore, it is vital to consider online behaviour in the context of the child' situation in general and any existing concerns. We use the same criteria as for any other Safeguarding concern in accordance with our Safeguarding and Child Protection Policy.

If a member of staff finds illegal content or potentially illegal content on the schools' network or a school owned device, you must immediately close the machine, secure the room or area and seek the advice of the Headteacher immediately.

The Headteacher should then contact the Head of Governance at the CYPES Department who will provide further advice and facilitate contact with the Police.

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

Images of Children (photos and video)

The school obtains parental consent to publish a picture of a child, whether on paper or online. Our consent forms are completed at the beginning of the child's school career and can last for the duration of their time at the school. However, a parent has the right to change their mind, and we record that decision.

Our consent form itemises different use of images, for example, use on school website, printing in local media, social media. If there is a 'one off' reason to publish a child's picture, then we would seek specific consent for that event. Once the press image has been captured with consent, the media organisation is then the data controller for that image.

Parents and carers can take pictures of their own children at their school provided it is for their own personal use and not uploaded to social networking sites.

Staff / volunteers can take pictures to support educational aims, but must follow school policies regarding the sharing, distribution and publication of those images. The images should only be recorded on school owned devices, not personal devices. Care should be taken that students are appropriately dressed and are not participating in activities that might bring the school into disrepute. Students must not take/use/share pictures of other students without permission.

Staff will actively teach pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet, and the need to gain consent before taking and uploading images of other people.

Data Protection and social media.

Care should be exercised when publishing pictures on social media. Even with permission from parents we do not provide more than two pieces of identifiable data, for example if the child is in school uniform and has their first name this counts as two pieces of data. Where possible we use generic or non-identifiable group pictures.

In situations where parents differ over consent, we will proceed as if no consent has been given (assuming both parents have legal parental responsibility).

Teaching about Online Safety

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

- A planned Online Safety curriculum should be provided as part of Computing / PSHE / other lessons and should be regularly revisited
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and pastoral 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- 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 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. The Online Safety Lead should be informed in case concerning searches appear in the following suspicious search log.

Acceptable Use Agreement

The school has a set of clear expectations and responsibilities for all users. This is outlined in the Acceptable Use Agreements. These are adapted for different user groups.