

Bedales School

Digital Safety Policy

INCLUDING EYFS

Implementation date: Autumn 2021

Date/term of last review: Autumn 2023

Author	DSL
Review body (individual or group)	Head of ICT, Bedales Senior Deputy Head Pastoral, DDSLs (Prep, Pre-Prep), Head of Wellbeing and PSHE of Prep, Senior and Coordinator at Pre-Prep; Head of Digital Learning, Senior.
Approval Body	WSST
ISI Regulatory Paragraph Number	7h
Next Review Period	Autumn 2024

Tick relevant box(es) ✓ how this Policy should appear:

Inspector Folder		✓
Website	Upload	✓
	Signpost	
Internal only		
Parent Portal		✓
For Students		✓

Bedales School Digital Safety Policy

Contents

Policy Aims	3
Scope.....	3
Links with statutory and non-statutory guidance, and other policies	4
Monitoring and review	4
Roles and responsibilities.....	4
Education and engagement approaches	6
Security and Management of Information Systems.....	7
Online concerns and identifiable risks	10
Responding to digital safety incidents and concerns	15
Appendix 1: Guidelines for Staff: Concerns about material on a student’s mobile phone.....	17
Appendix 2: Hampshire Constabulary’s Flowchart on managing Youth Produced Sexual Imagery (Nudes)	18

Bedales School Digital Safety Policy

Policy Aims

Access to electronic devices and the internet is an important part of everyday life. The use of School-owned and personal devices is supported at Bedales School, for both educational and recreational purposes, and the School has a duty of care to ensure its safe usage for students, staff and visitors.

This is the Bedales School Digital Safety Policy. Its purpose is to:

- safeguard and protect all members of the Bedales community online
- identify approaches to educate and raise awareness of digital safety throughout the community
- enable staff, visitors and students to work safely and responsibly, to demonstrate positive behaviour online and to maintain professional standards and practice when using technology; and
- identify clear procedures to use when responding to digital safety concerns.

Keeping Children Safe In Education KCSIE 2023 states that the management of digital safety can be broadly categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful material.

Contact: being subjected to harmful online interaction with other users.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Scope

Bedales understands that digital safety is an essential part of safeguarding and acknowledge our duty in ensuring all students and staff are protected from potential harm online.

Students should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all access to the internet and use of technology, including personal devices, and where students, colleagues and other individuals have been provided with School-issued devices for use off-site, such as work laptops, tablets and mobile phones.

This policy applies to all staff at the School (including the governing body, visitors and volunteers), as well as students, parents and carers.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents covered by this policy, which may take place outside the School, but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour 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 safety behaviour that take place out of School.

Links with statutory and non-statutory guidance, and other policies

This policy is informed by *Keeping Children Safe in Education 2023* as well as [Teaching online safety in schools](#); [Sharing nudes and semi-nudes: advice for educational settings working with children and young people](#), and [Searching, screening and confiscation at school](#), to be read in conjunction with Bedales policies (available online and on the intranet) including:

- The Bedales School Safeguarding and Child Protection Policy
- The Anti-Bullying policies for Bedales Senior, Prep and Pre-prep
- The Behaviour policies for the Bedales Senior, Prep and Pre-prep
- The ICT Acceptable Use policies for students and staff
- The Bedales School Data Protection Policy
- The Staff Code of Professional Conduct
- The PSHE and Wellbeing policies for Bedales Senior, Prep and Pre-prep

Monitoring and review

Technology in this area evolves and changes rapidly, so this policy will be reviewed on an annual basis. The policy will also be revised following any local or national changes to policy and procedure, any child protection concerns and/or changes to the School's technical infrastructure.

Internet use is always recorded and regularly monitored, and we will continue to evaluate the School's digital safety mechanisms to ensure this policy is consistently applied.

The Designated Safeguarding Lead will be informed of digital safety concerns, as appropriate.

The Designated Safeguarding Governor will report to the Board of Governors on digital safety practice and incidents, including outcomes, a regular basis.

Any issues identified via monitoring will inform our action planning.

Roles and responsibilities

The Designated Safeguarding Lead has lead responsibility for the management, training and reporting on digital safety as part of their wider lead responsibility for safeguarding and child protection at Bedales. All members of the School community have an important part to play when safeguarding children and young people, and a focus on digital safety is an important part of that remit.

Head and Governing Body

In conjunction with the DSL, the Head and Governing Body will:

- ensure that digital safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- ensure there are appropriate and up-to-date policies regarding digital safety, including the Schools' Behaviour policies, which cover acceptable use of technology
- ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks
- ensure that digital safety is embedded within a progressive curriculum, which enables all students to develop an age-appropriate understanding of digital safety
- support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their digital safety responsibilities
- ensure there are robust reporting channels for the community to access regarding digital safety concerns, including internal, local and national support

- ensure that appropriate risk assessments are undertaken and reviewed regarding the safe use of technology
- audit and evaluate digital safety practice to identify strengths and areas for improvement.

Designated Safeguarding Lead (DSL)

The DSL will:

- act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- ensure all members of staff receive regular, up-to-date and appropriate digital safety training
- access regular and appropriate training and support to ensure they understand the unique risks associated with digital safety and have the relevant and up-to-date knowledge required to keep students safe online
- access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online
- keep up to date with current research, legislation and trends regarding digital safety and communicate this with the community, as appropriate
- assist Houseparents in supporting students who are vulnerable to, or who have been exposed to, significant online harms
- signpost and initiate appropriate channels of referral where necessary
- ensure that digital safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- Work with the Network Managers to review the internet filters termly
- maintain records of digital safety concerns, as well as actions taken, as part of the School's safeguarding recording mechanisms
- monitor digital safety incidents to identify gaps and trends, and use this data to update the education response, policies, and procedures
- report digital safety concerns, as appropriate, to the Whole School's Strategic Team (WSST) and Governing Body
- work with the WSST to review and update digital safety policies on a regular basis (at least annually) with input from the Deputy DSL team, the Head of Wellbeing and PSHE of Bedales Senior, Prep, and Coordinator at Pre-Prep and the Head of ICT
- meet regularly (and at least annually) with the Designated Safeguarding Governor with lead responsibility for safeguarding and online safety.

Staff Members

It is the responsibility of all members of staff to:

- contribute to the development of digital safety policies
- read and adhere to the digital safety policy and ICT acceptable use policies
- take responsibility for the security of School systems and the data they use or have access to
- model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- embed digital safety education in curriculum delivery, wherever possible
- have an awareness of a range of digital safety issues and how they may be experienced by the students in their care
- identify digital safety concerns and take appropriate action by following the School's Safeguarding policies and procedures
- know when and how to escalate digital safety issues, including signposting to appropriate support, internally and externally
- take personal responsibility for professional development in this area.

It is the responsibility of staff managing the technical environment to:

- provide technical support and perspective to the DSL and Senior Leadership Team, especially in the development, implementation and review of appropriate digital safety policies and procedures
- apply internet filtering policies as set by the DSL or Senior Leadership Team, ensuring that the filtering policy is applied and updated on a regular basis (responsibility for its implementation is shared with the Senior Leadership Team)
- ensure that the monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the Senior Leadership Team
- ensure appropriate access and technical support is given to the DSL and the DCPC to the filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

Students

It is the responsibility of students (at a level appropriate to their age and ability) to:

- read and adhere to the ICT acceptable use policies annually
- respect the feelings and rights of others both on and offline
- take responsibility for keeping themselves and others safe online
- seek help from a trusted adult, if there is a concern online, and support others that may be experiencing digital safety issues
- engage in age-appropriate digital safety education opportunities
- contribute to the development of digital safety policies.

Parents/Carers

It is the responsibility of parents/carers to:

- read the ICT acceptable use policies and encourage their children to adhere to them
- support the School's digital safety approaches by discussing digital safety issues with their children and reinforcing appropriate and safe online behaviours at home
- conduct the necessary safeguarding checks on external tutors, counsellors and other professionals engaged to work with their children on School premises
- role-model safe and appropriate use of technology and social media
- identify changes in behaviour that could indicate that their child is at risk of harm online
- seek help and support from the School, or other appropriate agencies, if they or their child encounter risk or concerns online
- contribute to the development of the digital safety policies
- use School systems, such as learning platforms and other network resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and engagement approaches

The School will seek to promote and reinforce positive approaches to online behaviour and internet usage whenever possible in lessons. Teachers will seek to discuss online behaviours early and often, empowering students to recognise and report inappropriate, harmful or abusive content. The Wellbeing curriculum and the Prep School Digital Learning programme cover the following aspects of digital safety:

- staying safe online
- the effective use of the internet to research

- the skills of knowledge location, retrieval, and evaluation
- teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Bedales School will support students to read and understand the acceptable use policies in a way which suits their age and ability by:

- informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- providing digital safety education and training as part of the transition programme across the key stages and when moving between establishments
- seeking student voice when writing and developing digital safety policies and practices, including curriculum development and implementation using support, such as external visitors, where appropriate, to complement and support our internal digital safety education approaches.

Additionally, the School takes the following steps to protect and support its students:

- Acceptable use agreements for children and staff
- Regular updates and training for staff to ensure they can protect students
- Discussions between pastoral staff and students
- Information included in emails, letters/bulletin and the Parent Portal
- Pastoral sessions for parents
- Building awareness around information on websites and/or publications

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, referencing best practices and industry standards which include but not limited to

- Providing encryption functionality for staff for personal data sent over the internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems
- Encrypting local storage on any device where that functionality exists
- Not using portable media without specific permission; portable media can be checked by staff using an antivirus/malware scan before use
- Configuring the ICT estate to prevent the downloading of unapproved software to work devices or opening unfamiliar email attachments
- Implementing anti-virus and anti-spam systems on our email system
- Virus protection being updated regularly
- The ability to check files held on our network as required
- The appropriate use of user logins, passwords and best security practices such as multi-factor authentication to access our network
- Specific user logins and passwords enforced for all
- Applying appropriate access for staff to data stored on School systems.
- Utilising cloud-based systems
- Regularly deploying updates and security patches
- Utilising maintenance contracts to ensure systems are kept up-to-date and fully supported by suppliers
- Performing regular phishing tests, simulating a real-world phishing attack, enhancing staff awareness and training

- Subscribing to monitoring sites which perform industry standard security checks on our websites and alerts us to any issues

All users are expected to log off or lock their screens/devices if systems are unattended.

Reducing online risks

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via the School's computers or devices. However, we will:

- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the School is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Firewall and protection software

Levels of internet access are adjusted according to students' age and experience, and different filtering rules apply across Bedales, as well as across different year groups. We also adjust accessibility according to time of day and to allow for greater freedom when browsing at weekends.

The School uses firewall devices from Sophos to implement its filtering policies and protect the School's network from cyber threats, while FastVue produces usage reports for designated teachers to help identify any student internet of concern.

Sophos is only accessible by senior ICT staff (Network Managers and the Head of ICT) and they are responsible for configuring the Sophos firewall. Internet filtering rules (which define what sites and services are allowed or blocked) are defined by the School's Safeguarding and Senior Staff. The ICT department annually engage those staff to review and update the filtering rules.

FastVue automatically emails reports to Safeguarding Staff which highlight inappropriate activities by students. Staff can then login to FastVue to further interrogate the internet activity.

The DSL and Head of ICT also meet with students to review restrictions on specific sites.

Access to internet via non-School provided services, i.e. 4G and 5G

The School aims to educate students about safe internet usage, and our online filtering system ensures that problematic sites and social media platforms are blocked or restricted when accessed via the School's Wi-Fi or internet connection. Unfortunately, the School cannot control student internet access via non-School provided means such as mobile networks and therefore students can access any content via that method. We raise awareness with parents about 3G, 4G & 5G access and they have been asked to refrain from buying large data packages for their children. The School protects its students by minimising access to mobile phones and other devices in the younger years, and by promoting healthy device usage for older students.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation. Full information can be found in our Data Protection Policy.

Safer use of technology

Levels of online supervision will vary according to the age and level of experience for students across Bedales School.

As per the ICT Acceptable Use Policy, all students are required to set a personal password for their account and they may not share this information with other students.

Staff and student emails

All staff and students have a School email address which must be used in all School-related communication for safeguarding reasons.

Online lessons, hybrid learning and videoconferencing

All online lessons are conducted using Microsoft Teams. Staff must use School-issued devices for these lessons. Lessons are recorded and stored within the relevant Teams channels for safeguarding reasons.

Alongside all other expectations outlined in the Staff Code of Professional Conduct, colleagues and students should ensure:

- They, and any family members visible on-screen, are appropriately dressed
- Teaching takes place from 'public' spaces, i.e. from a space that is not obviously a bedroom
- Nothing inappropriate is seen or heard in the background. The 'blur background' function may be helpful in ensuring this
- Family members are not able to access any personal student data
- The language used is appropriate for the student, as well as other family members who may be within earshot
- Any non-timetabled contact (e.g. Tutor group 1:1s) take place during reasonable working hours (8am-5.30pm Monday-Friday; 8am-1pm on Saturdays - Bedales Senior only)
- Learning materials are age-appropriate; video links have been checked in advance.

Any further scheduled contact between staff and students should take place within mutually convenient times within the normal School working day and be organised and communicated to your line manager well in advance.

Any phone calls to students or parents are conducted using work mobile phones or through Teams; colleagues are not to disclose their personal phone numbers by calling students or parents.

Private online sessions

Skype, Zoom, Google Hangouts and other videoconferencing software is blocked by the School for safeguarding reasons. If parents wish their child to participate in sessions with outside tutors, counsellors, medical professionals and other practitioners they must complete the 'Additional use of School facilities for private online Tutoring and Counselling' form, which is available on the Parent Portal. We cannot conduct safeguarding checks on outside professionals, nor can we guarantee the safety of other videoconferencing platforms.

Social Media

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; Apps; video/photo sharing sites; chatrooms and messaging platforms.

All members of the Bedales community are expected to engage with social media in a positive, safe and responsible manner.

Inappropriate or excessive use of social media during School hours or whilst using School devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of the Bedales community on social media should be reported to the DSL and will be managed in accordance with our Safeguarding and Child

Protection Policy, the Staff Code of Professional Conduct, and the relevant Behaviour policies and Anti-Bullying policies.

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the School.

Online concerns and identifiable risks

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's Safeguarding and Child Protection Policy (available on the School website). Some such risks are identified below.

Cyberbullying

Central to Bedales Senior, Prep and Pre-prep Anti-Bullying policies is the principle that '*bullying is always unacceptable*' and that '*all students have a right not to be bullied*'.

The School responds to all bullying perpetrated in and outside school, and so we will respond to any cyberbullying we become aware of carried out by or against students when they are away from the site.

Cyberbullying is defined as "an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself." ([Peter K. Smith et al 2007](#))

By cyberbullying, we mean bullying by electronic media which may include, but is not limited to:

- Bullying by texts or messages, over social networks, or via any number of communication systems available over the internet
- The use of mobile phone cameras to cause distress, fear or humiliation (including the criminal offence of upskirting)
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- 'Trolling' using an anonymous username and account
- Outing or 'doxxing' – revealing personal information about someone – including information about their sexual orientation - online for malicious purposes
- Distributing personal material against someone's wishes
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums.

This type of bullying has a greater impact on the victim when there is an element of repetition and a real or perceived power imbalance between the victim and the perpetrator(s).

Cyberbullying and the law

Cyberbullying may be at a level where it is criminal in character. It is unlawful to disseminate defamatory information in any media including internet sites.

- Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
- Section 1 of the Malicious Communications Act 1988 makes it an offence to send another person electronic communication which is threatening or the sender believes to be false in order to cause distress or anxiety.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

If we become aware of any incidents of cyberbullying, we will need to consider each case individually as to any criminal act that may have been committed. The School will pass on information to the police if it feels that it is appropriate or are required to do so. We will always inform parents beforehand unless this would present a risk to the student(s).

Radicalisation

'Radicalisation is usually a process, not an event', Prevent strategy document.

Young people are at risk of encountering individuals online who may express extreme views. These propagandists may seek to promote their views in an attempt to radicalise susceptible individuals. These susceptible individuals are disproportionately young people.

There are various terror groups seeking to recruit individuals to their cause. These include, but are not limited to:

- Far right extremists
- Islamic fundamentalists
- Republican groups in Northern Ireland

Some factors may make an individual more susceptible to radicalisation, including:

- The search for identity, meaning and community, which they may not have found in their 'real world' environment
- Feeling apparent or real discrimination in their 'real world' environment
- Sympathy and association with a terrorist 'value system', 'community' or apparent 'just cause'

Propagandists are able to reach susceptible individuals via the internet using video clips, social media groups, chat rooms and through propaganda distributed on websites.

Terrorist groups target individuals who sympathise with their cause in order to build rapport and isolate individuals from mainstream views. By developing an online social group they can nurture increasingly extreme points of view within the group which ultimately leads to radicalisation.

These groups can encourage communication via the dark web or via encrypted messaging services so it becomes more difficult for agencies to trace and find individuals. The dark web is also used to point individuals to extreme illegal content that would be taken down by legitimate hosting companies.

The School will provide a developmentally appropriate Wellbeing and PSHE curriculum in order to ensure that students are aware of the dangers of radicalisation, and will work closely with students who are identified as potentially more vulnerable to radicalisation. Pastoral staff at Bedales will alert the Designated Safeguarding Lead or Deputies if they have concerns about a child's vulnerability to radicalisation. Concerns about online material promoting terrorism or extremism will be reported on the Gov.UK Report Terrorism website.

Sharing Youth Produced Sexual Imagery (YPSI)

Sharing videos, 'selfies' and pictures is part of everyday life for young people, but the taking and sharing of nude images is illegal, risky and potentially damaging on a number of levels for young people. It constitutes a criminal offence (Protection of Children Act 1978, as amended by the Sexual Offences Act 2003). While sharing nude images is not an uncommon occurrence, NSPCC research has shown that most young people aren't sharing sexual imagery of themselves.

Students are not permitted to use the School network to have, take, make or share an image in any medium of themselves, or another student at School, or anyone else under the age of 18, which shows breasts or genitalia or suggests a sexual act. Students should discuss plans for any work that may involve a state of undress with the relevant teacher, usually within Art and Design.

The guidance on defining and responding to YPSI is taken from Hampshire Constabulary's Risk Assessment advice and *Sharing nudes and semi-nudes: advice for education settings working with children and young people*

This guidance refers specifically to images that have been taken by children under the age of 18, and shared with other children under the age of 18.

Bedales School's initial aim is to educate young people on the dangers of this practice through Wellbeing sessions, in assemblies and in other contexts.

Any member of staff who becomes aware of an indecent image should take the following steps (outlined in Appendix 1):

- Confiscate any device where an image is present, ensuring it is switched to 'flight mode', or turned off
- Do NOT view the image or take steps to share it electronically
- Report the matter to the DSL immediately
- **The DSL will meet with those concerned to assess the risk factors, which include the children's ages and circumstances, following Hampshire Constabulary's risk assessment advice flowchart**
- A decision will be made about how to proceed, which may include contacting police, social services and other agencies for further advice or to make a referral,
- The process will be discussed with parents (unless it is deemed unsafe to do so)
- Ongoing support will be offered to the young people involved.

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to students involved and the risks can be managed within the School's pastoral support and disciplinary framework and, if appropriate, their local network of support.

If a member of staff receives a youth-produced sexual image on any device, they must delete the image immediately and report the matter to the police and to the DSL.

Sharing nude images for malicious purposes

Sharing nude images of children without consent is both illegal and abusive. The distribution of sexual imagery for malicious purposes or without consent will be reported to the social media platform on which it has been shared, to CEOP and/or to children's services. Staff will handle any disclosures of this kind with sensitivity and discretion, supporting the young people in question as well as their families. Bedales Senior, Prep and Pre-prep Behaviour and Anti-Bullying policies and procedures will be adhered to when addressing issues of this nature.

Online Child Sexual Exploitation (OCSE)

Online Child Sexual Exploitation (OCSE) includes the online communication between an adult and a child for the purpose of sexual exploitation. It sometimes involves grooming of children over a period of time in order to gain their trust. Perpetrators may rely on threats, intimidation and coercion in order to deceive victims into engaging in sexual activity online. OCSE can also lead to offline offending, such as meetings between an adult and a child for sexual purposes.

The School will work with students and their families if they are found to be victims of OCSE, and will take advice from CEOP, Hampshire Police and Children's Services as part of this process.

Online Child Criminal Exploitation (CCE) and Child Financial Exploitation (CFE)

Child Criminal Exploitation is where an individual or group takes advantage of an imbalance of power to coerce, control, manipulate or deceive a child into any criminal activity a) in exchange for something the victim needs or wants or b) for the financial or other advantage of the perpetrator or facilitator and/or c) through violence or the threat of violence. The victim may have been exploited even if the activity appears consensual. While CCE can occur through physical contact, it can also take place through the use of technology.

This can include acting as 'money mules' or 'squaring' – making use of their bank account to move money on behalf of a criminal gang.

Unexplained gifts or new possessions; going missing from school, home or a care setting; the misuse of drugs or alcohol, or spending time with people who are known to engage in exploitation can be indicators that a child is vulnerable to CCE.

Grooming¹

Online grooming is the deliberate action by a predatory adult of preparing a child or vulnerable person for a meeting. Children are vulnerable to grooming in online platforms and games that allow them to communicate with people they do not know.

The School will build awareness amongst children and parents about ensuring that the child:

- Only has friends online that they know in real life
- Is aware that if they communicate with somebody that they have met online, that relationship should stay online.

That parents should feel empowered to:

- Recognise the signs of grooming
- Have regular conversations with their children about online activity and how to stay safe online.²

The School will raise awareness by:

- Include awareness around grooming as part of their curriculum
- Identifying with both parents and children how they can be safeguarded against grooming.

Gaming

Online gaming is an activity that the majority of children and many adults get involved in. Risks include accessing graphic and age-inappropriate material; grooming or cyberbullying through online chat functions; addiction; revealing passwords, bank details or other sensitive information.

The School will raise awareness of the potential risks associated with this by:

¹ <http://www.childnet.com/search-results/?keywords=grooming>

<http://www.internetmatters.org/issues/online-grooming/>

² <https://www.internetmatters.org/hub/parent-stories/making-friends-and-managing-real-friendships-online-tips-from-a-parent/>

- talking to parents and carers about the games their children play and help them identify whether they are appropriate
- monitoring gaming sites and other online platforms via our internet filtering system and restricting access to certain games which are deemed to be risky
- supporting families in identifying the most effective way of safeguarding their children by using parental controls and child safety mode
- communicating to parents and carers about setting boundaries and time limits when games are played
- highlighting relevant resources.

The Dark Web

The Dark Web is a term used to describe a small section of the internet which is not accessible via standard internet searches such as Google or Bing. The Dark Web offers the person viewing, and the websites that they view, total anonymity. This area is only accessible using a special web browser which encrypts any Dark Web information across multiple layers, providing the anonymity.

The anonymity afforded by access to the dark web has been exploited by those wishing to evade legal jurisdictions, and it therefore poses a safeguarding risk by allowing unfiltered access to sites pertaining to extremism, extreme pornography, dealing in arms and drugs, extreme violence and other elements that are otherwise restricted by law.

Accessing the Dark Web is considered a serious misuse of the School's ICT infrastructure, and we will follow the School's Behaviour policies in managing issues relating to this. The School will review issues relating to the use of the Dark Web on a case-by-case basis, working openly with the police and other agencies to ensure that we maintain transparency and support any victims of criminal activity.

Use of personal devices and mobile phones

Bedales School recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within the School.

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti-Bullying, Behaviour, Child Protection and Safeguarding, and ICT Acceptable Use Policy. Staff must not use personal devices for any School-related activity or business unless specifically mentioned in the ICT Acceptable Use Policy.

Personal electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the Bedales community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

Members of staff are not permitted to use their own personal phones or devices for contacting students or parents/carers. Any pre-existing relationships, which could undermine this, will be discussed with the DSL. Where possible, i.e. when not using 2FA, staff at the Prep School are also asked to keep their mobile phones in their bags or in a cupboard. They are asked to use personal devices in the staffroom or in another space designated for staff use, e.g. an office.

School mobile phones and devices will always be used in accordance with the relevant policies. Staff will not use personal devices:

- to take photos or videos of students; and will only use work-provided equipment for this purpose

- directly with students and will only use work-provided equipment during lessons/educational activities

If a member of staff breaches our policy, action will be taken in line with our Code of Conduct/Staff Behaviour Policy.

Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences. Rules and expectations regarding mobile phone usage will vary according to the time of day and the situation.

Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our Behaviour or Anti-Bullying policies or could contain youth produced sexual imagery (sexting). The following would apply:

- Searches of mobile phone or personal devices will only be carried out in accordance with our Behaviour and Safeguarding & Child Protection policies
- Students' mobile phones or devices may be searched by the On-Call staff member or another member of the Senior Leadership Team, with the consent of the student or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our Behaviour and Safeguarding & Child Protection policies
- Students are expected to provide any codes to allow the search of their device to be performed where there is a valid reason for doing so
- Mobile phones and devices that have been confiscated for these reasons will be released to parents/carers
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Responding to digital safety incidents and concerns

If staff or students discover unsuitable sites then the URL, time, date and content must be reported to the Head of ICT or a member of the Safeguarding Team. Any content that is found to be unlawful will be reported to the relevant agencies, either by the Safeguarding Team, the Head of ICT or an IT Network Manager.

Students at Bedales School will be supported, listened to and taken seriously when reporting incidents or concerns.

Procedures for responding to specific online incidents or concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Students, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents/carers and students to work in partnership to resolve online safety issues. After any investigations are completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Hampshire Children's Reception Team.

If an incident or concern needs to be passed beyond our community (for example if other local schools are involved or the public may be at risk), the DSL will speak with Hampshire Police and/or the Children's Reception Team first to ensure that potential investigations are not compromised.

The DSL will be informed of any online safety incidents involving Safeguarding or Child Protection concerns and will record these issues in line with our Safeguarding and Child Protection policies.

The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Hampshire Safeguarding Children's Board thresholds and procedures.

The DSL will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

Any complaint about staff misuse of technology will be referred to the DSL and/or the Head of ICT. Appropriate action will be taken in accordance with our Safeguarding and Child Protection Policy, our Staff Code of Professional Conduct and the Safeguarding Allegations Procedure.

Allegations regarding a member of staff's online conduct will be pursued in accordance with the Bedales Safeguarding Allegations Procedure and discussed with the Local Authority Designated Officer (LADO) if appropriate.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police and other relevant agencies will be contacted.

NB: All School Policies are available to staff and can be found here:

T:\ThreeSchools\Policies_Handbooks_Key_Documentation\Staff_viewable

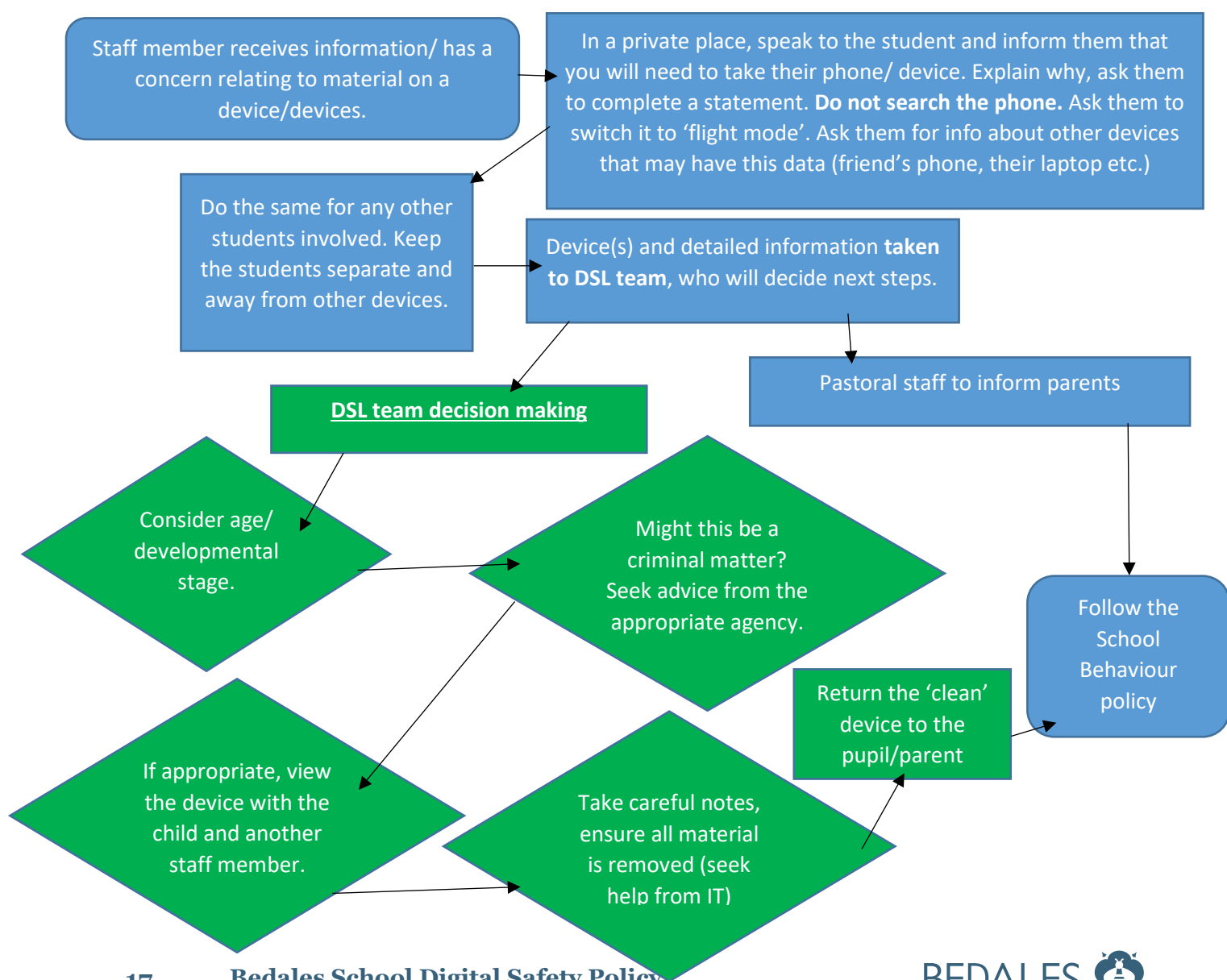
Appendix I: Guidelines for Staff: Concerns about material on a student's mobile phone

Guidelines for staff: concerns about material on a student's mobile phone

These guidelines should be referred to if there are concerns about material on a student's mobile phone, including (but not limited to) the following:

- Online bullying
- Nude or semi-nude images
- Supplying or distributing drugs or other illegal substances or materials
- Material which may compromise or embarrass a student or staff member
- Evidence of OCSE/CSE
- Any other illegal content

All colleagues should feel confident in following these steps if there are concerns of this nature.




Appendix 2: Hampshire Constabulary's Flowchart on managing Youth Produced Sexual Imagery (Nudes)

YOUTH PRODUCED SEXUAL IMAGES (YPSI) AND INAPPROPRIATE SEXUAL CONTACT ONLINE

Risk assessment advice to safeguard children and young people

A QUICK GUIDE



Call the police on 101

As part of Hampshire Constabulary's commitment to working in partnership with education to keep young people safe and informed, it is important we ensure that education partners and practitioners have a clear picture of the force approach to dealing with cases of YPSI and inappropriate sexual contact online.

This information aims to support schools and partners dealing with cases of YPSI or sexual contact online to determine the need to report to police for investigation or whether matters can be dealt with outside of the law by staff, the young people involved and parents, respecting that a police response will not always be necessary.

Yes

DO ANY OF THESE FACTORS EXIST?

The presence of any aggravating factors means the matter should be reported to police to safeguard those involved and investigate the case further.

- These involved are under 13yrs?
- An adult aged 18 or over is involved?
- Multiple victims/wider distribution
- The level of sexual nature/type of image
- Threats/coercion/harassment present
- Grooming or exploitation expected
- Wide age gaps in relationship cases

No

Where an incident has no aggravating factors, police intervention is not necessary, the matter should be resolved by staff in a balanced and proportionate way in accordance with their own safeguarding policies.

Images produced (as part of or within) a consensual relationship for romantic or affection-seeking reasons with no identifiable aggravating factors

- Victim/suspect are **not** at high risk of CSE or other abuse and vulnerabilities
- No further/persistent contact from suspect
- Contact and conversation appear to be age appropriate
- Images only distributed between each other
- Type of image sent – nature/tone

Can I look at the image or content?

Only if it is completely necessary to make a full risk assessment. Conduct only with given permission from relevant staff according to school or your organisation's protocol, unless it is considered in the presence of someone else at school. This is procedurally and accurately.

Can I seize a child's phone?

Yes you can. This may be necessary for the safety of the child to reduce the risk of harm from content being shared or distributed and to make a full risk assessment.

Can I give the child's phone back to them?

Yes. If your risk assessment determines the case is low risk and falls under the expedited route, contact parents and agree whether they require the child to hand their phone back. All images held on that is then recorded in school/guardian records. Do not give the child the phone back until the risk has been done.

Will calling the police mean the child will get a criminal record?

Hampshire Constabulary will not seek to create a young person, their safety and welfare is always the priority.

Only in serious cases would the police have to consider formal sanctions.

What do I do if the image is sent to me?

Delete it immediately, do not retain it, show it to others or share it. Report this to your manager and the police.

What if parents aren't happy with our decision not to call the police?

Ensure parents are informed why and that they have the option to make a report themselves.

Record your investigation, assessment and details to enable police to support you if a report is made that we need to respond to.

18

Bedales School Digital Safety Policy

BEDALES 