Digital Safety Policy

Stowe School
Independent Boarding and Day School for Boys and Girls

Policy Reviewed: September 2023
Policy Review Date June 2024
Policy Owner: Group Director of ICT
Version: V43

Table of Contents

Revision History

The following table should be updated throughout the lifetime of this document:

Version	Date	Details	Author
V09	18/1/12	First Draft	NJM
V12	25/2/12	Needs input from SMT, needs Inset in 3 strands- IT, Pastoral, esafety Officer.	NJM
V13	2/4/12	Changes to e-safety and photos policy	NJM
V14	22/4/12	Changes to 'responsibilities for esafety section- removed e-safety officer as requested	NJM
V15	24/4/12	Added further detail to e-mail section	NJM
V17	19/5/12	Amended reporting of DP incidents	NJM
V18	3/02/14	Updated social media section to exclude use of social media and to exclude mobile phone use	NJM
V19	12/14	Updated social media section 3.10 with new safeguarding material	KJM
V27	9/1/15	Amended e-safety committee structure and adapted reporting to reflect changes in management structure- safeguarding. Deputy Head responsibilities amended. Amended incident reporting.	NJM
V28	6/5/15	Amended 3.3 to reflect Firewall posture regarding extremism.	NJM
V29	22/9/15	Added Parental AUP reference, 3rd 4th form device night storage/safe policy.	NJM
V30	6/12/16	updates to sections 2.7, 3.11 and 3.12	KJM
V31	3/2/17	Clarify new position concerning prevent legislation, bring min age of SNS staff joining to Alumnus to 21	NJM
V34	10/5/17	Annual review Crispin Robinson / James Peppiatt. Changed reporting procedures, document name from e-safety. Redefined esafety committee members.	NJM
V35	7/9/17	Reformatted numbering. Inserted changes to mobile device times as per James Peppiatt request, and added HM role in publishing	NJM
V36	10/9/17	Changed reporting procedure for incidents	NJM
V37	23/2/18	Updated references to technical terms	
V38	24/4/19	Update references to DSL / DDSL KCSIE 2018 Annex C – training.	CCR
V39	25/4/19	Boarding House section formatted to allow publication in Houses as directed by Deputy Head (Pastoral). New DP policies referred to in section 3.8.	NJM
V40	22/4/21	Changed job role titles to reflect new job titles and of ELT members, added section 5	NJM
V43	1/9/23		EH/AG

Distribution

This document has been distributed to:

Name	Purpose	Version	Date
Second Master	Amend/Update in accordance with School's requirements	V09	18/1/12
ELT	Clarify purpose, Shape the policy, allocate responsibilities and timing of inset/training	V12	25/2/12
All staff	Introduced only staff safety elements during INSET.	V15	24/4/12
Assistant Head/Senior Housemaster Pete Last	Review pastoral elements prior to rollout	V15	27/4/12
All Staff	Published on intranet	V17	19/5/12
DSL	Amend policy on safe mobiles Internet and SNS site use & safeguarding update	V18	2/1/14
DSL		V30	2/12/16
All staff	Published on VLE	V38	1/9/18
Governors		V39	25/4/19
Senior Deputy Head, DSL, HOD ICT	Approved for publication of 2021 policy	V41	14/5/21
Senior Deputy Head, DSL, HOD ICT	Approved for publication of 2022 policy	V42	June 2022
ELT	Approved for publication of 2023 Policy	V43	01/09/23

1. Digital Safety

1.1 Other Policies

Many of these risks reflect situations in the off-line world and it is essential that this Digital Safety Policy is used in conjunction with other School policies, these include:

> The Stowe Staff Code of Conduct, the visitor's code of conduct, the Safeguarding and Child Protection Procedures and Policies Booklet, the anti-bullying policy and the School pupil behaviour and disciplinary policies.

1.2 Background

The development and implementation of this policy involves all the stakeholders in a pupil's education from the Headmaster to the House Staff, Classroom Teachers, Support Staff and parents as well as the pupils themselves.

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. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. The School Digital Safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in schools and boarding houses has been shown to raise educational standards and promote pupil achievement. Some of the dangers from within and outside the School include:

- Access to illegal, harmful, or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information (DPA)
- 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 those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

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 Safety 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) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1.3 Development / Monitoring / Review of this Policy

Members of the Pastoral Committee will:

- review/monitor the School digital safety policy/documents (including AUPs, Security Policies etc.)
- review/monitor the School filtering/firewall policy

This Digital Safety policy will be developed by the School's Pastoral Committee which is made up of:

- Senior Deputy Head
- Group Director of ICT
- Deputy Head (Pastoral)
- Deputy Head (Pastoral) and DSL
- Safeguarding Supervisory Governor(s)

Consultation with the whole School community will take place through the following:

- Staff meetings and INSETS
- Stoic Council
- INSET Day as part of the safeguarding update and training
- School website / Intranet
- Publication of regulations on House noticeboards

The School will monitor the impact of the policy using:

- Logs of reported incidents
- Logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys
- Pupils
- Parents
- Staff

1.4 Scope of the Policy

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

The Education and Inspections Act 2006 empowers the Head to such extent as is reasonable, to regulate the behaviour of pupils when they are off the School site and empowers members of staff to follow

disciplinary procedure for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Digital Safety incidents covered by this policy, which may take place out of School, but is linked to membership of the School.

The School will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents of incidents of inappropriate Digital Safety behaviour that take place out of school.

2. Roles and responsibilities

The following section outlines the roles and responsibilities for Digital Safety of individuals and groups within the school. KCSIE (2023 Annex) provides the most up to date Guidance for Online Safety:

2.1 Governors

The Governors are responsible for the approval of the Digital Safety Policy and for reviewing the effectiveness of the policy (in conjunction with other pastoral policies).

2.2 Assistant Deputy Head (Pastoral) and DSL

The Senior Deputy Head / DSL, working with the Group Director of ICT, is responsible for:

- the Digital Safety of pupils through the oversight of the development of relevant training and policy.
- reviewing online safety specific training and have an "up-to-date capability required to keep children safe whilst they are online".
- DDSLs should be in line with DSL re online safety specific training and setting out that the role should be explicit in any job description.
- ensuring that relevant staff receive suitable training to enable them to carry out their Digital Safety duties and to train other colleagues, as relevant.
- advising concerning serious Digital Safety incidents that require disciplinary aspects (as per the Behavioural Policy).
- a member of the Pastoral Committee.
- taking day to day responsibility for pupil Digital Safety issues and taking a leading role in establishing and reviewing the Schools' pupil Digital Safety policies / documents.
- ensuring that all staff are aware of the procedures that need to be followed in the event of a Digital Safety incident which involves pupil safety.
- appropriate reporting to ELT concerning the above.
- ensuring that Data Protection events are forwarded to the Privacy Officer for recording in the Data protection log.

The Deputy Head (Pastoral) & DSL will inform, Group Director of ICT and HR in the event of a serious Digital Safety allegation being made against a member of the academic staff. The DSL is trained in Digital Safety issues and is aware of the potential for serious safeguarding and child protection issues to arise from:

- Youth Produced Sexual Images (sexting- e.g. Sharing nudes/Semi Nude images and/or videos)
- sharing of personal data (DPA)
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming

- cyber-bullying

It is important to emphasise that these are safeguarding and child protection issues, not technical issues simply that the technology provides additional means for safeguarding and child protection issues to develop. ELT will receive Digital Safety reports as appropriate from the Deputy Head (Pastoral).

2.3 The Senior Deputy Head

The Senior Deputy Head will forward personal data related incident details to the Privacy Officer for recording in the log.

2.4 The Group Director of ICT

Is a part of the school ELT regular discussing current issues, review incident logs and filtering / change control logs and receive reports of all incidents and to inform future Digital Safety developments in order to ensure:

- that the School's ICT infrastructure is secure and adequately protected from misuse or malicious attack
- that the School meets the Digital Safety technical requirements outlined in the School's Security Policy and Acceptable Usage Policy
- users may only access the School's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the School's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he / she keeps up to date with Digital Safety technical information in order to effectively carry out their Digital Safety role and to inform and update others as relevant
- that the use of the network / intranet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Deputy Head (Pastoral) and DSL / HR manager or other members of ELT
- that monitoring software / systems are implemented and updated as agreed in School policies.
- the IT Department are fully briefed with the relevant areas of the Digital Safety and other IT policies.

2.5 Deputy Head (Pastoral)/DSL

The DH (Pastoral)'s responsibilities include:

- Ensuring all House Staff have an up-to-date awareness of Digital Safety matters and of the current School Digital Safety policy and practices with particular attention to issues specific to boarding houses.
- Making sure that House Staff are aware of their role in Enforcing the AUP/Digital Safety policy in particular relating to pupil devices in boarding houses and informing the Assistant Deputy Head (Pastoral) and DSL of any breaches.
- Monitoring of ICT use, where practical, in boarding houses.
- Making sure that House Staff are actively engaging with Pupils in their House to make them understand the issues with regard to Digital Safety.

- Taking opportunities to engage parents in making them understand the potential risks with regard to Digital Safety.
- Holding a review meeting with the Privacy Officer to update Digital Safety policy with reference to the incident log.

2.6 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of Digital Safety matters and of the current School Digital Safety policy and practices
- They have read, understood and signed the School Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Group Director of ICT / Deputy Head (Pastoral) and DSL for investigation / action / sanction
- Digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official School systems such as e-mail unless authorised by the Senior Deputy Head or Group Director of ICT.
- Digital Safety issues are embedded in all aspects of the curriculum and other School activities
- Pupils understand and follow the School Digital Safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor IT activity in lessons, extra-curricular and extended School activities
- They are aware of Digital Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current School
- policies as laid out in the School planner with regard to these devices
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that accidental incidences of inappropriate content occurring will be reported to the IT dept.

2.7 Pupils

The pupils' responsibilities include:

- Using the School IT systems in accordance with the Pupil Acceptable Use Policy, adopting safe practices, which they will be expected to confirm, during an induction class, that they have read and understood it before being given access to School systems. See the latest copy of acceptable-use-policy
- Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Keeping a backup on school systems including One Drive, of vital files and work
- Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Knowledge and understanding the School policies on the use of mobile phones, digital cameras and hand held devices

- Knowledge and understanding of School policies on the taking / use of images and on cyber-bullying
- An understanding of the importance of adopting good Digital Safety practice at all times when using digital technologies and to realise that the School's Digital Safety Policy includes their usage when outside the boundaries of the school.

2.8 Parents

Parents 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 do not fully understand the issues and are less experienced in the use of IT than their children. Parents are given and asked to sign a parental AUP to clarify their responsibilities in keeping pupils safe in the use of technology.

3. Policy Statements

3.1 Curriculum

- Digital Safety should be a focus in all areas of the curriculum and staff should reinforce Digital Safety messages in the use of IT across the curriculum
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- 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
- 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

3.2 Staff Training

- It is essential that all staff receive Digital Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- It is expected that some staff will identify Digital Safety as a training need within the performance management process
- All new staff should receive Digital Safety training as part of their induction programme, ensuring that they fully understand the School's Acceptable Usage Policy (AUP)
- The Group Dierctor of ICT will organise training advice/guidance to individuals or groups as required
- Staff will all receive 'Online Safety' training via educare once a year.

3.3 Digital Safety Education

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

Digital Safety education will be provided in the following ways:

- A planned Digital Safety programme will be provided as part of PSHE lessons and should be regularly revisited and tested – this will cover both secure use of IT and new technologies in School and outside School.
- Key Digital Safety messages are reinforced as part of a planned programme of tutorial / pastoral activities.

- Pupils will 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 Pupil AUP and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside School.
- Within lessons, pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet will be posted in all ICT rooms.
- Rules relating to the use of ICT in boarding houses will be displayed on boarding house notice boards. A Digital Safety notice/poster will be supplied for this purpose.
- Staff should act as good role models in their use of IT, the internet and mobile devices.

3.4 Pastoral Use of ICT Equipment

Pastoral care is fundamental to Stowe's boarding environment; the School's pastoral policies demonstrate Stowe's commitment to providing pupils with the highest level of pastoral care. This pastoral care also extends to ICT, both school provisioned and increasingly pupil-owned computing devices (laptops, mobile/smart phones, PDAs, word processors) as well as peripherals such as monitors, printers, special keyboards, mice and games consoles of all varieties. Pupils also are very keen to connect those devices to the internet via a variety of methods: via mobile 4G or by attempting to connect them to the School's network.

For these reasons there needs to be some specific guidance for House Staff on ICT devices pupils bring into House (pupils will be informed of these policies in the AUP). Parents will be informed using the Parent Acceptable User Agreement. 3rd and 4th and 5th form pupils must hand in their devices before 2nd prep and bedtime.

3.5 Cyber-bullying

Cyber-bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007.

Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, School staff and parents understand how cyber-bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. Stowe School recognises that cyber bullying is in all likelihood running concurrently with face-to-face bullying.

Cyber-bullying (along with all forms of bullying) will not be tolerated in the School. Full details are set out in the School's policy on anti-bullying.

Sanctions for those involved in cyber-bullying are the same as any other form of bullying (as per the behaviour policy but will also include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at School for the user for a period of time.
- Confiscation of mobile devices whilst at School.
- If Safeguarding concerns are raised this could lead to suspension or expulsion.

3.6 Using Email

- Email is regarded as an essential means of communication and the School provides all members of the School community with an e-mail account for School based communication- texting and other methods are not 'auditable' and can be taken out of context.
- Communication by email between staff, pupils and parents should only be made using the School email account and should be professional and related to School matters only. E-mail messages on School business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the School is maintained. There are systems in place for storing relevant electronic communications which take place between School and parents.
- Use of the School e-mail system is monitored and checked.
- As part of the curriculum, pupils are taught about safe and appropriate use of email.
- Pupils are informed that misuse of email will result in a loss of privileges.
- Responsible use of personal web mail accounts by staff is permitted.
- Protocols are in place to ensure staff are restricted in their use of mass emails.
- Where non-School e-mail addresses are used staff should use the BCC (blind copy) address bar to keep the e-mail addresses private. If the address bar is not visible this should be enabled using the options menu.
- Care should be taken to ensure that content is sent to the appropriate recipient, with special regard to the information contained in previously forwarded parts of the email.

3.7 Technical – infrastructure / equipment, filtering and monitoring

- Also see Information Security Policy and Taking and Using Images of Children 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Digital Safety responsibilities.
- School IT systems will be managed in ways that ensure that the School meets the Digital Safety technical requirements outlined in the School Security Policy and Acceptable Usage Policy.
- There will be annual reviews and audits of the safety and security of the School IT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will be provided with a username and password by the IT department who will keep an up to date record of users and their usernames. Users will be required to change

their password according to the network password policy. This is enforced by the Network every 6 months and should not be updated according to a recognisable pattern.

- Users will be made responsible for the security of their username and password, and should also use physical security (locked doors/drawers) to restrict access to computers. User's 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, for example unknown devices attached to the computer.
- The IT Department maintains and supports the managed internet filtering and firewall service and includes proxy sites, VPN services, unethical sites and extremism within
- the categories that are excluded under specific educational filters from an industry standard perspective. Please inform IT if any sites are permitted that pose a threat to pupils or staff at Stowe.
- In the event of the IT Department needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head of ICT.
- School IT technical staff, in collaboration with teaching and Pastoral/House staff and the DSL, monitor and record the activity of users on the School IT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by the IT Department to control workstations and view users' activity and this will only be done with the knowledge and consent of the user of that computer.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the School's systems and data.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the School system.
- The School infrastructure and individual workstations are protected by up to date virus software (continuously updated throughout the day) and are patched for all available critical security vulnerabilities (during holidays and half terms).
- Personal data must not be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

3.8 School website

The School maintains editorial responsibility for any School initiated website or learning platform content to ensure that content is accurate and the quality of presentation is maintained. The School maintains the integrity of the School website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact for the website is the School address, e-mail and telephone number. Published contact details for staff are School provided.

Creating online content as part of the curriculum:

As part of the curriculum, we encourage pupils to create shared digital content. Pupils are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a wide range of audiences within the Stowe community which might include Governors, parents or

younger children. Blogging, podcasting and other publishing of online content by pupils for School related activities should take place within a protected forum. Appropriate procedures to protect the identity of pupils must be followed.

Publishing personal information over the internet should only be undertaken with the permission of the Senior Deputy Head and Privacy Officer. School sponsored content sharing should be moderated by the responsible teacher to avoid publication of any inappropriate or personal material. To enable effective and safe use of content sharing, a Stowe intranet web page or the Stowe VLE or a site that offers the option of teacher moderation is the best solution to protect the School community from inappropriate content being published, including pictures or video as detailed below.

3.9 Managing School Networking Sites (SNS) and their use by pupils and staff

Sections 3.8 & 3.9 should be read in conjunction with the Safeguarding and Child Protection Policy

Social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All pupils are advised to be cautious about the information given by others on SNS sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, School details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the School.
- Staff may only create blogs, wikis, forums or other web 2 spaces in order to communicate with pupils' systems approved by the Pastoral committee.
- Staff who make private use of Social networking are given the following advice:
    - Always adopt and maintain the appropriate privacy settings
    - Avoid 'friending' pupils or past pupils (or relatives of pupils) on their private accounts
    - Always maintain professional standards o Never post anything unprofessional
    - Never post School or pupil information / photographs without permission from the School and the pupils' parents
    - Warn friends of the dangers of posting incriminating photographs or information

3.10 Safeguarding and Child Protection Staff Conduct: Social Media and Mobile Devices

Sections 3.8 & 3.9 should be read in conjunction with the Safeguarding and Child Protection Policy

All Stowe School staff must ensure that personal social media accounts such as Facebook, Instagram, Twitter et al are protected with robust security settings. The settings should ensure that pupils cannot access personal photographs, friend lists, 'likes' and written posts should not be available to the public. Staff should never allow pupils to befriend or 'follow' them on any social media account whilst a staff member is employed by Stowe School.

In addition, Staff may only create blogs, wikis, forums or other web spaces in order to communicate with pupils' systems approved by the Pastoral committee. All Staff are expected to always maintain professional standards (Staff Code of Conduct) and never post School or pupil information or images on their personal accounts.

In order that staff are protected from allegations of 'grooming' or inappropriate contact with pupils, staff are requested to decline contact with ex pupils via personal social media accounts until the alumnus has reached the age of 21.

3.11 Mobile devices

A 'mobile device' may be a phone, ipad, ipod or iphone or any form of hand held phone, tablet or laptop with the facility to take photographs and transmit them electronically and/or to hold conversations or personal video recorders and cameras.

Staff are reminded that The Protection of Children Act 1978 prohibits at Section 1(1)(a) the "taking or making" of an indecent photograph or pseudo-photograph of a child. According to the Memorandum of Understanding between Crown Prosecution (CPS) and Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003:

"Making includes the situation where a person downloads an image from the internet or otherwise creates an electronic copy of a file containing such a photograph or pseudo photograph. To be an offence such a 'making' must be a deliberate and intentional act, with the knowledge that the image made was, or was likely to be, an indecent photograph or pseudo photograph of a child."

Personal mobile devices cannot be used to record classroom activities – only school property can be used for this purpose. Photographs may be taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements, however it is essential that photographs / film are taken and stored appropriately to safeguard the children in our care. Images can only be transferred to and stored on a school computer to be printed. Parental consent is sought for photographs to be taken or published i.e., on the school website or in publications. Care must be taken by staff to ensure that any photographs or images of pupils does not identify any individual child by name in a publication to be shared with the public. During trips and visits - school provided mobile phones are available from Reception. For health and safety on school trips, a staff trip leader's mobile number can, with their consent, be distributed to pupils, however staff must not reciprocate and store pupil's mobile phone numbers in their personal devices. Staff must report any inappropriate communications from pupils to staff personal mobile phones to the Assistant Deputy Head (Pastoral) and DSL immediately.

It may be necessary in a school boarding environment for some staff other than Housemasters (e.g., Tutors, Masters in charge, sports staff) to be informed of a 6th Form pupil's personal mobile number.

When this is necessary, pupils should be asked to email their mobile number to the member of staff concerned via the Stowe School server/outlook. Staff must ensure that pupils' mobile numbers are **never** stored in their personal mobile contact list. Contact via personal mobile must only contain work related communication and always use professional language. Should a member of staff receive communication considered inappropriate they must **immediately** inform the Assistant Deputy Head (Pastoral) and DSL.

3.12 Process for Staff when discovering indecent images of pupils

Staff need to be particularly careful when discovering incidents of Youth Produced Sexual Images (YPSI) as it is possible that a staff member may breach the law and could themselves be accused of making or sharing indecent images of children.

If any member of staff (including support staff such as IT staff) finds an indecent image of a child, they should follow this procedure:

- If the image is on the School network, staff must alert ICT Support on internal phone: 8296/8234 who will disable access to the area where the picture(s) have been stored.
- The image(s) should not be viewed during this process.
- If the image(s) is on a pupil owned device or network, staff must confiscate the device.
- Staff must not view the material beyond the first initial identification of an indecent image if the staff member finds the image by accident or is sent the image unknowingly. Staff must never screenshot or forward the image.
- If a pupil discloses to a staff member in respect to a YPSI they must ask the pupil to describe the image but not view it themselves. The DSL must be contacted, pupil devices confiscated, and ICT Support alerted immediately if the image is on a network/public social media page.
- The Deputy Head (Pastoral) and DSL will be notified by ICT Support. If the image is on a device this should be kept securely and delivered by hand to the Deputy Head (Pastoral) and DSL.
- The Deputy Head (Pastoral) and DSL will document a Digital Safety 'incident' on MyConcern.
- MASH and in all likelihood, the Police will be informed and advice followed from them.

Following an investigation by the Deputy Head (Pastoral), DSL and Head, following the procedures as stated in the Safeguarding and Child Protection Policy, the image will be removed from the network/device. If an image is on a pupil's social media page (or other external web site) – this will be deleted by the pupil under supervision.

3.13 Protecting School Data

Personal data will be recorded, processed, transferred, and made available according to the GDPR Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes

- Adequate, relevant, and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

More specific detail on data protection can be found in the School's data protection policies and procedures.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse by keeping them on school storage whenever possible.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When handling printed copies of personal data from the School's MIS systems, those printouts are secured against loss and shredded when no longer required.

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

- The data must be encrypted, and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with School policy (as set out in the security policies and procedures) once it has been transferred or its use is complete.

4. Data Protection Incident Reporting, Digital Safety Incident Log & Infringements

4.1 Incident Reporting

Any incident involving a pupil must be reported to the pupil's Housemaster/mistress who will then deal with the incident following the Digital Safety incident process (detailed at 4.3 below).

4.2 Incident Log

All Digital Safety incidents concerning Data protection will be reported to Privacy Officer by the Assistant Deputy Head (Pastoral) & DSL and then recorded in the Digital Safety log which will inform the development of policy at the summer Digital Safety review meeting.

4.3 Process for handling Digital Safety Incidents

In incidents involving a pupil either as victim or originator of the incident please refer to the safeguarding policy and follow the appropriate procedure.

4.4 Possible sanctions in case of Digital Safety breach by a pupil

This is a suggested guide for House Staff who need to sanction a digital Safety offence.

First offence (depending on the incident)	Loss of email for 1-3 weeks Loss of internet access for 1-3 weeks Loss of Smartphone*/iPod/iPad for 2days Loss of computer in Study for 1 week (any work for Preps would require a visit to the library) Any other sanction common to a particular boarding house for minor offences
Second offence	As above (but Sanctions included) + Detention (with a particular focus on Digital Safety…) Letter to parents
Third offence (or serious breach)	As Above (but Sanction period until the end of term…)

	Suspension.

5. Additional Links provided by the Government in KCSIE 2021:

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on sexting-inschools-and-colleges, using-external-visitors-to-support-onlinesafety-education and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.

5.1 Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

6. Boarding House IT Safeguarding Regulations

This notice is a part of the Digital Safety Policy which details regulations for safe use in Boarding Houses in addition to the Acceptable Usage Policy which is available on the Stowenet at https://stowe.fireflycloud.net/pupil-it-help/acceptable-use-policy

Information below re-enforces the fact that the School firewall filters and logs all attempts to access unsuitable web sites. Also social media website are switched off at unsuitable times, and in any event all Wireless access is turned off after 11.30pm. Full details of network access arrangements are on Stowenet at:

https://stowe.fireflycloud.net/pupil-it-help/network-wireless-and-internet-access-times

Hacking or any attempts to avoid any restriction below, or any unsuitable use of technology as a serious breach of privacy can result in confiscation of phones, a letter home and sanctions being applied by Housemasters. More detailed advice is at section 4 of the Digital Safety Policy.

Item	Pupil regulation	Background notes
Mobile Devices/ Smart phones / iPods /MP3 players	Pupils are allowed mobile phones / Smartphones / iPod, MP3 players in boarding houses, but these are subject to the School's Acceptable Use Policy.	Parents are warned about the possible Digital Safety risks that these devices present through the Parental Acceptable use policy and asked to restrict pupil devices to an appropriate level. Pastoral care and safeguarding education to promote responsible use are therefore paramount additional layers of pupil safety. Pupils are educated about the Digital Safety risks these devices present (as part of the School's safeguarding program).
Laptops / Tablet devices	Pupils are allowed to bring in their own Laptops or Tablet devices and access various services using Stowenet and Office 365. To access the network they must install a Virus checker and update and then pass through the School network access security procedure. All 3rd form pupils will use school provided digital device with appropriate safeguarding software	Parents are warned via the Parental Acceptable Usage Policy of the possible Digital Safety Risks that these devices present and need for their cooperation in managing risks effectively. It is important to note that any device bought into School will need to be covered by parents' insurance policy and pupil's need to observe appropriate security precautions to safeguard their property under the terms of that policy. The School will maintain no liability for the loss or damage to these devices.
Connectivity of pupil owned devices	Pupils are only allowed to connect their devices to the School network through a specific wireless network, StoweNSL, configured by the IT department for that purpose.	Any attempts to avoid filtering using external networks or VPN will result in immediate confiscation of the device and may necessitate a return of the device to the parent with a letter explaining the issue.

	Connectivity of a pupil owned device to the internet via 5G/4G, or non-School wireless devices is NOT ALLOWED if an alternative School provisioned wireless service is available in Houses.	Any hacking attempt from the device will be considered a serious breach of the rules as it has the potential to significantly disrupt the School's operation.
Pupil owned Wireless network devices	Pupils are NOT ALLOWED to bring in equipment that will broadcast any wireless connection within the boarding house.	Pupils will attempt to do this to bypass the School's internet filter. Any devices found will be confiscated immediately.
Network usage times	All network access is restricted for the use of SNS during teaching, prep and after lights out.	Devices that are used or switched on out of these times will be confiscated for a period as defined by the Housemaster. If a pupil is using Social Media during prep or lesson times, it is likely they are using a 5G/4G network or bypassing the School filters.
Peripherals for School PCs	• Pupils are allowed to use the following peripherals on School machines: • Standard USB Mice and Keyboards (Note IT will not install device specific drivers for particular models). • Private Printers and computer monitors are not allowed to be connected to School machines. Devices that draw power via USB connectivity (such as mini fridges, desk fans etc.) are not allowed.	USB transfer of data to the School network is permitted as long as it is scanned by an updated virus checker.
Games Consoles	Pupils are not allowed to bring games consoles into a House. Handheld gaming devices are allowed but will only be used within the boarding house (see further note about excessive use).	Any console found will be confiscated and sent home at the earliest opportunity with a suitable notification to parents.

Storage or Downloading of inappropriate material	Downloading or storage of inappropriate or offensive material on pupil-owned devices is not allowed.	If such material is discovered, then confiscation of the device will be required and material will need to be cleaned and removed (the IT department will help in this process and investigate the method through which the materials were accessed). Serious breaches will be followed up by the Senior Master with parents.
The taking, storage or transmission of indecent images or any information of pupils or staff is prohibited.	The making, storage or transmission of indecent images or information regarding pupils or staff is not allowed and is seen as serious breach of the School rules.	In the event of finding such an image, follow the 'Process for staff handling indecent images of pupils' within the School Digital Safety Policy. Failure to follow the correct procedure could lead to Police involvement.
Inappropriate use of images, videos or films.	The taking and or viewing of inappropriate images (photos, videos or films/DVDs) in house is not allowed. In any event pupils should not take photos of other pupils or staff without permission or if they are in any way intrusive of their privacy.	Examples of inappropriate material include videos of fights/pranks, films/ DVDs and viewing materials with a certificate that is inappropriate to the age of the child. Recording should not take place in any form in changing rooms, showers toilets or other private spaces.
Using a device for the purposes of causing distress to others (Cyber bullying)	Cyber bullying is when a person, or a group of people, uses the internet, mobile phones or other digital technologies to threaten, tease or abuse someone. This is not tolerated and will be handled using the AntiBullying policy.	Any suspected cyber bullying is likely to result in the device being confiscated. Please see section 3.5 to 4.4 of the Digital Safety Policy for further advice.
Unauthorised or secret use of personal devices	Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is not allowed. Unauthorised publishing of such material on a web site which causes distress to the person(s) concerned will be	Please see section 3.6 to 4.4 of the Digital Safety Policy for further advice.

	considered a breach of School discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.	
On-Line gambling.	On-line gambling on any devices is not allowed.	If evidence of on-line gambling is found there will be a suitable punishment by the housemaster and a letter sent home to parents.
Gaming on personal devices.	Excessive gaming on personal devices and hand held gaming devices is not allowed.	If a pupil is excessively gaming and this is affecting their contribution to the house or academic studies, then the device will be confiscated for a period stipulated by the Housemasters / Housemistresses. ICT can be requested to reduce bandwidth available to pupils.
Video / Online meetings	On-line meeting tools such as Skype, FaceTime are not blocked on pupil devices unless such use results in bandwidth usage which causes issues to the normal running of network services at Stowe.	The Assistant Deputy Head (Pastoral) and DSL, and Housemaster should be alerted of any safeguarding concerns resulting from inappropriate use. Please see section 3.6 to 4.4 of the Digital Safety Policy for further advice.