SHEBBEAR COLLEGE

E-SAFETY POLICY

Whole School Policy

Reviewed and Updated: 1st September 2022 by F Lovett & C Banyard
Reviewed by SLT: February 2023
Next Review: February 2024

Policy Review at Shebbear College

The SLT acknowledge their responsibility to ensure that this policy is effective and follows regulatory requirements. The SLT and Governors undertake a regular review (at least annually) to satisfy themselves that the implementation of this policy is effective.

1. Introduction and Overview

1.1 Scope of the policy

Shebbear College is committed to promoting and safeguarding the welfare of all pupils and an effective online safety strategy is paramount to this. The policy applies to all members of the College community (staff, students, volunteers, parents, carers, and visitors) who have access to and are users of the College's ICT systems.

For clarity the e-safety policy uses the following terms unless otherwise stated:

- **Users** – Refers to staff, governors, volunteers, pupils, and any other person working in or on behalf of the College, including contractors.

- **Parents** – Any adult with legal responsibility for the child/young person outside of the College e.g. parent, guardian, or carer.

- **College** – Any College business or activity conducted on or off the College site, e.g. visits, College trips, conferences, etc.

- **Wider College community** – Pupils, all staff, governing body, and parents.

The College utilises technology and the internet extensively across all areas of the curriculum. E-safety is described as a College's ability to safeguard, protect and educate pupils and staff in the acceptable use of technology and communications (including social media) as well as having established mechanisms in place to identify, intervene and escalate any incident where appropriate. The area is evolving constantly and as such this policy will be reviewed on an annual basis or in response to an e-safety incident whichever is sooner.

1.2 The purpose of this policy is to

- Outline the guiding principles of all members of the College community regarding the use of ICT.
- Safeguard and protect the students and staff helping them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other College policies.
- Ensure that all members of the College community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

The policy is to ensure the requirement to empower the whole College community with the knowledge to stay safe and risk free. All risks are identified and mitigated (where possible) in order to reduce any foreseeable harm to the user or liability to the College.

2. Review and Monitoring

2.1 Safeguarding Committee and Governing Body

The safeguarding committee and governing body are accountable for ensuring that the College has an effective e-safety policy and procedure in place. As such they will review this policy at least annually and in response to any e-safety incident ensure that the policy is up to date, covers all aspects of technology use within the College. Ensure e-safety incidents are appropriately dealt with and ensure that the policy is effective in managing such incidents.

2.2 Senior Deputy Head (Pastoral) and Digital Learning Lead

- The Senior Deputy Head (Pastoral) and Digital Learning Lead have a wider remit in overseeing and managing e-safety incidents. They will also report to the governing body as required.

The Senior Deputy Head (Pastoral) and Digital Learning Lead will ensure that:

- All e-safety incidents are dealt with promptly and appropriately and are logged using CPOMS.
- E-safety training throughout the College is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team, governing body and parents.
- All staff have had appropriate CPD in order to effectively support e-safety.

3. Roles and responsibilities

3.1 Senior Deputy Head (Pastoral) and Digital Learning Lead

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for College and home use, for example, through attendance of the National Online Safety courses, webinars and updates etc.
- Review this policy regularly and bring any matters to the attention of the Head.
- Advise the senior leadership team and governing body on all e-safety matters.

- Engage with the wider College community on e-safety matters at College and/or at home.
- Liaise with the local authority, ICT technical support and other agencies as required.
- Ensure staff know that all e-safety incidents should be reported using the College's safeguarding platform, CPOMS.

3.2 ICT Technical Support

ICT technical support are responsible for ensuring that the ICT technical infrastructure is secure; this will include as a minimum:

- Ensure any technical e-safety measures in College (e.g. internet filtering software, behaviour management software) are fit for purpose.
- Anti-virus is fit for purpose, up to date and applied to all capable devices.
- Operating systems are regularly updated.
- Any e-safety technical solutions such as internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed with the Deputy Head Pastoral and the Head.
- Passwords are applied correctly to all users regardless of age.

3.3 All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Senior Deputy Head (Pastoral).
- Remain familiar with current trends and issues surrounding e-safety. (There is no expectation for staff to be 'experts', but they should have a working understanding of the key social media platforms, privacy settings, potential pitfalls and how to respond to an e-safety incident, for example being aware of how to deal with an incident involving youth produced sexual imagery).
- Seek support, advice and guidance from the Digital Learning Lead if they feel their knowledge and understanding of online-safety issues need refreshing.
- Report any suspected or known e-safety incident via CPOMS. Once reported it is passed to the DSL for action.
- They are aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.
- All digital communications with pupils, parents or carers should be on a professional level and only carried out using official College systems.
- In lessons, where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and staff should report incidents involving unsuitable material that is found in internet searches to the Senior Deputy Head (Pastoral).
- Any concerns about a potential breach of security or system should be reported immediately to the ICT Technical Support.

3.4 All Pupils

Pupil owned mobile devices, such as, smartphones, tablets and laptops have the ability of utilising the College's wireless network. The device also has access to the wider internet and other cloud based services such as email and data storage via G Suite. All pupils should understand that, during the course of the normal College day, the primary purpose of their device in a College context is educational. Boarders are permitted to use their devices for non-educational purposes outside of the normal College day. If there is reason to believe a pupil is misusing the privilege of having access to the College systems or internet the College reserves the right to access their accounts and in necessary suspend their access.

The boundaries of use of ICT equipment and services is given in the Acceptable Use Statement; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at College or outside of College and are encouraged to report any known misuse of mobile technology especially relating to cyber-bullying.

3.5 Parents and Carers

Parents play the most important role in the development of their children; as such the College will support parents in understanding and acquiring the skills and knowledge they need to ensure the safety of children outside the College environment. Parents are kept up to date with new and emerging e-safety risks via the National Online Safety portal.

Parents must also understand the College needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will support the College in its application of Acceptable Use.

3.6 The Safeguarding Committee

Chaired by the Senior Deputy Head (Pastoral), e-safety will fall within the remit of this committee:

- Advise on changes to the e-safety policy.
- Establish the effectiveness (or not) of e-safety training and awareness in the College.
- Recommend further initiatives for e-safety training and awareness at the College

4. Conduct and Incident Management

4.1 Conduct

All users are responsible for using the College ICT systems in line with the Acceptable Use Statement and they should understand the consequences of misuse, or accessing inappropriate materials.

All members of the College community should know that this policy also covers their online activity outside of College if it relates to their membership of the College.

4.2 Incident Management

All members of the College community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively, in line with the College’s policies. The College actively seeks advice and support from external agencies in handling online safety issues. Parents and carers will be informed of any online safety incidents relating to their own children, unless doing so may put the child at risk. All parents and carers will receive more general online safety advice in response to incidents, without revealing any sensitive or personal information about students.

4.3 Technology

Shebbear College uses a range of devices including PC's, laptops, Chromebooks and Apple Macs. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

- **Internet Filtering** – The College uses Smoothwall to prevent unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Online-Safety Advisory Team is responsible for ensuring that the filtering is appropriate and that any significant issues are brought to the attention of the Head Master. The use of filtering avoidance products such as VPNs, are strictly forbidden. Any deliberate attempts to avoid internet filtering will lead to a disciplinary response determined by the SLT.

- **Email Filtering –** Provided by GSuite (Gmail) it mitigates against infected email being sent to the College. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email and phishing emails. If a message is received which potentially contains malware or phishing content the message may be automatically quarantined by the system. Users should familiarize themselves with phishing prevention practices.

- **Encryption –** All College mobile devices that hold personal data (as defined by GDPR 2018) are encrypted. No data is to leave the College on an un-encrypted device. Any breach (i.e. loss/theft of device such as laptop or USB key drives) is to be brought to the attention of the 78iujkm Head immediately. The Head will liaise with the ICT team and Digital Learning Lead to determine what course of action should follow.

- **Passwords –** all staff and pupils will be unable to access the College's internet without a unique username and password. The password policy requires staff and pupils to use a strong password and guidance is updated and provided regularly by the ICT Team and Digital Learning Lead. Passwords have an expiration period of 90 days. If a password is compromised the user must change the password and inform the ICT team or Digital Learning Lead immediately.
- **Anti-Virus –** All capable devices will have anti-virus software. This software, provided by Sophos, is updated at least hourly for new virus detection. ICT Team will be responsible for ensuring this task is carried out, and will report to the Head if there are any concerns. All USB peripherals such as key drives are scanned for viruses upon connection.

5. Data

The College has a Data Protection and Handling Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; the responsibilities of the Compliance Officer and the storage and access of data. The Data Protection and Handling Policy has been reviewed and updated since the introduction of the EU GDPR and the Data Protection Act (2018). There is guidance outlining when and how staff may use their own devices for work purposes and this includes the handling of personal data and sensitive information.

6. Education and Curriculum

The College has a clear e-safety education programme primarily as part of the PSHE curriculum but referenced in all areas of College life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy
- Acceptable online behaviour
- Understanding of online risks
- Privacy and security

- Reporting concerns

6.1 The College will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities using the Acceptable Use Agreement.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.

6.2 Safe Use

Internet – Use of the Internet in College is a privilege, not a right. By logging onto the College network each pupil or member of staff, volunteer or guest with access are automatically committing to abide by the Acceptable use policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and GDPR regulations, as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted.
Pupils are permitted to use the College email system, and as such will be given their own email address and they must confirm to accept e-mail protocols.

The College also reserves the right to access a user's email account if there is reason to believe the account is being used inappropriately.

Photos and videos – Every new parent has the choice of opting out of allowing the College to use their child's image/s when they receive and sign the College's Terms and Conditions.

7. Social Media

7.1 Digital and Video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital and video images to support educational and marketing aims, but must follow College policies concerning the taking, sharing, distribution and publication of those images. All staff are given guidance on the College's policy on taking, using and storing images of children.
- Staff should, whenever possible, use College cameras/recording devices rather than personal equipment. **NB**. Staff working with children in the EYFS must not use personal recording equipment at any time.

- If using personal devices, staff should transfer all materials as soon as reasonably possible to a College device and delete all materials from their personal devices/s.
- Digital images of pupil must be stored secured securely on the Shebbear College Marketing Drive.
- Digital images of pupils should not be stored on personal/home computers/hard drives, except where these images have been publicly available to parents or others on the College's website or in the weekly newsletter. It is acceptable to have play or team photographs for instance.
- Hard copies of children's images should be stored securely on the College premises, except where these are used for publicity purposes around the College: e.g. team and play photographs.
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be in keeping with the College's social media guidance.
- Pupils' full names will not be used on the College website and on social media platforms.

7.2 Social Networking – there are many social networking services available; the College is supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider College community. The College has accounts for Twitter, Instagram and Facebook which are managed by the College marketing department.

In addition, the following is to be strictly adhered to:

- There is to be no identification of pupils using first name and surname; first name only is to be used. Tagging to personal accounts is not permitted.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the College are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy - should it come to the College's attention that there is a resource which has been inadvertently uploaded, and the College does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any online-safety incident is to be brought to the immediate attention of the Senior Deputy Head (Pastoral), or in their absence the Deputy Head (Academic).

Training and Curriculum - It is important that the wider College community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, the College will provide regular updates and training suitable to the audience.
Online-safety for pupils is embedded into the curriculum; whenever ICT is used in the College, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The Senior Deputy Head (Pastoral) is responsible for recommending a programme of training and awareness for the school year to the Head for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Senior Deputy Head for further CPD.

8. Youth produced sexual imagery

The practice of children sharing images and videos via text message, email, social media or mobile messaging apps has become commonplace. However, this online technology has also given children the opportunity to produce and distribute sexual imagery in the form of photos and videos. Such imagery involving anyone under the age of 18 is illegal.
Youth produced sexual imagery refers to both images and videos where:

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18.
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult.
- A person under the age if 18 is in possession of sexual imagery created by another person under the age of 18.

All incidents of this nature should be treated as a safeguarding concern and in line with the UKCCIS guidance ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’[1].

Cases where sexual imagery of people under 18 has been shared by adults and where sexual imagery of a person of any age has been shared by an adult to a child is child sexual abuse and should be responded to accordingly.

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647389/Overview_of_Sexting_Guidance.pdf