



SHEBBEAR COLLEGE

ONLINE SAFETY POLICY

Whole College Policy

Reviewed and Updated: September 2025 by R Giles

SLT: September 2025

Next Review: June 2026

Policy Review at Shebbear College

The Governors 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.

Introduction and Overview

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 online 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. Online safety is described as the 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 this policy will be reviewed annually or in response to an online safety incident, whichever is sooner.

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 pupils 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, 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.

Review and Monitoring

Safeguarding Committee and Governing Body

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

Senior Deputy Head and Digital Learning Lead

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

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

- All online safety incidents are dealt with promptly and appropriately and are logged using CPOMS.
- Online 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 online safety.

Roles and responsibilities

Senior Deputy Head 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 College 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 online safety matters.
- Engage with the wider College community on online 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 online safety incidents should be reported using the College's safeguarding platform, CPOMS.

ICT Technical Support

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

- Ensure any technical online 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 online safety technical solutions such as internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; those categories of use are discussed with the Deputy Head Pastoral and the Head.
- Passwords are applied correctly to all users regardless of age.
- Ensure all students and staff appear on the data management and administration system, identifying that the devices are compliant and not utilising DNS proxy servers, VPNs or equivalent methods of bypassing the College's network security.

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.
- Remain familiar with current trends and issues surrounding online 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 online 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 online 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.
- Any concerns about a potential breach of security or system should be reported immediately to the ICT Technical Support.

All Pupils

Pupils from Form 1-5 are provided with a College managed device which should be used for educational purposes. The College managed device is monitored for acceptable use, in line with the acceptable use policy. If pupils wish to use their own devices in Sixth Form; the pupils are able to access the College network via the secured Wi-Fi connection and are still subject to the acceptable use policy.

Pupil owned mobile devices, such as smartphones, tablets and laptops have the ability of utilising the College's wireless network. Pupils have access to the wider internet and other cloud-based services such as email and data storage via Microsoft Office 365. 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 are 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.

Online safety is embedded into our curriculum; pupils will be given 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.

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 online safety risks via the National College 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.

The Safeguarding Committee

Chaired by the Senior Deputy Head online safety will fall within the remit of this committee:

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

Conduct and Incident Management

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.

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.

Technology

Shebbear College uses a range of devices including Surface Pro's, Surface Go's, PC's, laptops, Chromebooks, iPads 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 unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate are 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. 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 Microsoft Office 365 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 Senior Deputy 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. The 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.
- **Key strokes** - monitoring is used to monitor inputs on Devices and flag any potential Safeguarding key terms or words. This is then flagged using Smoothwall and sent for monitoring.

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.

Education and Curriculum

The College has a clear online 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

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.

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.

Social Media

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 pupils 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 a 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.

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 X (formerly 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 license 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.

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 for 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 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.

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 of 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'.

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.

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

If a member of staff becomes aware of an incident involving youth produced sexual imagery, they should follow the child protection procedures and refer to the DSL as soon as possible. The member of staff should confiscate the device involved and set it to flight mode or, if this is not possible, turn it off. Staff should not view, copy or print the youth produced sexual imagery.

The DSL should hold an initial review meeting with appropriate College staff and subsequent interviews with the children involved (if appropriate). Parents should be informed at an early stage and involved in the process unless there is reason to believe that involving parents would put the child at risk of harm. At any point in the process if there is concern a young person has been harmed or is at risk of harm a referral should be made to MASH or the Police as appropriate. Immediate referral at the initial review stage should be made to MASH/Police if:

- The incident involves an adult.
- There is good reason to believe that a young person has been coerced, blackmailed or groomed or if there are concerns about their capacity to consent (for example, owing to special education needs).

- What you know about the imagery suggests the content depicts sexual acts which are unusual for the child's development stage or are violent.
- The imagery involves sexual acts.
- The imagery involves anyone aged 12 or under.
- There is reason to believe a child is at immediate risk of harm owing to the sharing of the imagery, for example the child is presenting as suicidal or self-harming.

If none of the above apply then the DSL will use their professional judgement to assess the risk to pupils involved and may decide, with input from the Head, to respond to the incident without escalation to MASH or the police.

In applying judgement, the DSL will consider if:

- There is a significant age difference between the sender/receiver.
- There is a significant age difference between the sender/receiver.
- There is any coercion or encouragement beyond the sender/receiver.
- The imagery was shared and received with the knowledge of the child in the imagery.
- The child is more vulnerable than usual i.e. at risk.
- There is a significant impact on the children involved.
- The image is of a severe or extreme nature.
- The child involved understands consent.
- The situation is isolated or if the image has been more widely distributed.
- There are other circumstances relating to either the sender or recipient that may add cause for concern i.e. difficult home circumstances.
- The children have been involved in incidents relating to youth produced imagery before.

If any of these circumstances are present the situation will be escalated according to our child protection procedures, including reporting to the police or MASH. Otherwise, the situation will be managed within the College.

The DSL will record all incidents of youth produced sexual imagery, including both the actions taken, actions not taken, reasons for doing so and the resolution in line with safeguarding recording procedures.

ADVICE TO STAFF

Searching a device

- In a school-based context, it is highly likely that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device: it may be on a website or on a multitude of devices; it may be on either a College-owned or personal device.
- If any illegal images of a child are found the police will be informed immediately.

Never:

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the pupil/young person UNLESS there is clear evidence to suggest that

there is an immediate problem.

- Print out any material for evidence.
- Move any material from one storage device to another.

Always:

- Confiscate and secure the device(s).
- Inform the DSL.
- Record the incident.
- Act in accordance with College safeguarding and child protection policies and procedures.

Containing the incident and managing student reaction

There are cases in which victims of youth produce sexual imagery have had to leave or change schools because of the impact the incident has had on them. The pupil will be anxious about who has seen the image and where it has ended up. They will seek reassurance regarding its removal from the platform on which it was shared. They are likely to need support from the College, their parents and their friends. Creating a supportive environment for students in relation to the incident is very important and staff should be vigilant and report any further concerns after an incident has occurred.

Generative AI

Purpose

This policy sets the expectations and safeguards for using generative AI tools by students and staff. It supports educational innovation while ensuring compliance with statutory safeguarding guidance under **KCSIE 2025**.

2. Scope

Applies to all staff, students, volunteers, and external partners using any generative AI technology—on-site, remotely, during school hours or otherwise.

3. Alignment with KCSIE 2025

- **Online Safety & Content Risk**

Under Part 2 of KCSIE 2025, the scope of online safeguarding harms now explicitly includes **misinformation, disinformation, and conspiracy theories** (para 135) [services4schools.org.uk/NSPCC Learning](https://services4schools.org.uk/NSPCC-Learning). Users should remain vigilant about the credibility and origin of AI-generated content and ensure it is verified before use.

- **Filtering, Monitoring & AI Guidance**

KCSIE 2025 references the DfE’s “**Plan Technology for Your School**” self-**assessment tool** (para 142) and adds links to **Generative AI: Product Safety Expectations** (para 143) services4schools.org.uk/SmoothwallKeoghs. Use of AI tools must conform to these DfE technical and safeguarding expectations.

- **Safeguarding Responsibility**

Any alert or suggestion generated by AI—including safeguarding flags—must always be **reviewed by a qualified human**. Decisions should not be taken solely based on AI output [gine.com](https://www.gine.com).

4. General Principles

- **Human Oversight:** AI outputs must be reviewed and approved by staff before being shared or applied in learning environments or safeguarding contexts.
- **Transparency:** Users must disclose when content has been AI-generated.
- **Educational Alignment:** AI tools should support the curriculum and pedagogy, not replace them.
- **Accuracy & Source Verification:** Always cross-check AI-generated content against reputable sources.
- **Data Privacy & Safety:** AI tools must comply with data protection law (UK GDPR) and not expose personal or sensitive information.

5. Staff Responsibilities

- Only use AI tools approved by school leadership and confirmed to meet **DfE product safety expectations**.
- Review AI outputs before incorporating into lesson materials; ensure content is age-appropriate and factually correct.
- Act as a “human-in-the-loop”: You are responsible for verifying, editing, and contextualising AI-generated material.
- Report concerns—fake news, inappropriate or harmful AI content—via safeguarding channels.
- Engage parents/guardians in conversations about AI safety, mirroring guidance in KCSIE about parent communication [gine.com](https://www.gine.com).

6. Student Guidelines

- Use AI tools only when authorised and supervised.
- Label any AI-generated work (e.g., “Created with AI assistance”) to ensure transparency.
- Critically assess AI outputs—question reliability, bias, and content suitability.
- Never submit AI-generated content as entirely original work.

7. Approved AI Tools & Access

- The school will maintain a list of approved AI applications, vetted against DfE standards and safeguarding protocols.
- Regular reviews of these tools will occur to ensure compliance with **KCSIE 2025** and evolving guidance.

8. Monitoring & Enforcement

- Filtering and monitoring systems—assessed via the DfE’s tool—must continuously block harmful content, including AI-generated misinformation or extremist material [EdTech Innovation HubDISA](#).
- Use of AI in contravention of policy may result in disciplinary action, in line with the school’s safeguarding and behaviour policies.

9. Review & Future Updates

- The policy will be reviewed annually or when significant changes occur in DfE guidance, especially guidance on **RSHE** and **gender-questioning children**, expected to be included in final **KCSIE 2025** in September 2025 [services4schools.org.ukTes](#).

10. Key Terms Defined

- **Generative AI:** Systems that can create text, images, or other media content (e.g. ChatGPT, AI-assisted lesson creators).
- **Human-in-the-loop:** A practice where AI outputs are always reviewed and contextualised by qualified humans—never used unvetted.
- **Misinformation/Disinformation/Conspiracy Theories:** Newly recognized online safeguarding risks per KCSIE 2025 (para 135).

Acceptable Use Statement

This policy outlines what are acceptable and unacceptable uses of Information Communications Technology (ICT) facilities within Shebbear College. It is relevant to pupils, staff, governors and visitors. Whilst we aim to support the full use of the vast educational potential of new technologies, we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect pupils, staff and visitors from online safety incidents and promote a safe e-learning environment for pupils.

At Shebbear College we believe that pupils should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our College.

Acceptable use

- Shebbear College's ICT facilities should only be used to support learning, teaching, research, administration and approved business activities of Shebbear College during the College Day. These services may not be used for personal commercial, political, charitable, and other such activities unless expressly authorised by Shebbear College.
- Should authorisation be provided permitting other personal, personal commercial, political, or charitable, any such use must not hinder or interfere with an individual's duties and must not prevent the legitimate use of these facilities by others. Users may not use Shebbear College's ICT facilities to store personal non-work-related information or materials on the ICT facilities (e.g. eBooks, music, home videos, photography), and use of the ICT facilities is provided with no expectation of privacy.
- Users should therefore engage in safe computing practices by establishing appropriate access restrictions for their accounts by setting a password for their user account, safeguarding their passwords, backing up files, and promptly reporting any misuse or violations of this policy.
- Users' accounts and passwords must not be shared with anyone. Users are responsible for the security of their passwords, accounts and setting account and file permissions. Disclosure of account or password information may result in disciplinary action.

Monitoring of users

- Shebbear College may monitor the usage of any or all IT facilities and has access to reports on any internet sites that have been visited. This is irrespective of whether it is for Shebbear College or personal use, and users should have no expectation of privacy when accessing or using IT systems or services.
- Monitoring of ICT facilities is performed:
 - To monitor the performance and operation of the ICT facilities.
 - To secure, fix, enhance or as an inherent part of effective and responsible systems development or operation.
 - To collect evidence pertaining to compliance with this policy, and other related policies, regarding the acceptable use of ICT facilities within the College.
 - To investigate or detect unauthorised use of the computing and network facilities of Shebbear College.
 - In the interests of national security, as required by law and to prevent or detect crime, as required by law.
- Shebbear College reserves the right to inspect any items of computer equipment connected to

the network. Any ICT device connected to Shebbear College's network will be removed if it is deemed to be breaching College policy or otherwise interfering with the operation of the ICT facilities.

- Shebbear College will designate Authorised Personnel, usually IT services or support staff, to be permitted to engage in monitoring and it will be considered a disciplinary offence for anyone to engage in monitoring activities without proper authorisation or monitor areas outside their areas of responsibility.

Unacceptable use

Shebbear College reserves the right to block, disconnect or otherwise prevent what it considers to be unacceptable use of its ICT facilities. Unacceptable use includes, but is not limited to:

- All actions or activities that are illegal or in conflict with Shebbear College's policies, procedures and processes.
- Using the ICT facilities for access, creation, modification, storage, download, hosting or transmission of material that could be considered pornographic, offensive, obscene, or otherwise inappropriate, or for placing direct or indirect links to websites which publish or host pornographic, offensive or inappropriate material.
- Publishing materials or making statements which Shebbear College may deem to be advocating illegal activity, or threatening, or harassing, or defamatory, or bullying or disparaging of others, or abusive, or libelous, or slanderous, or indecent, or obscene, or offensive or promotes unlawful discrimination, breaches copyright or otherwise causing annoyance, or inconvenience.
- Unauthorised production, distribution, copying, selling, hiring, performing of copyrighted material including, but not limited to, digitisation and distribution of computer software, television, radio, streaming services, websites, photographs, magazines, books, music or any copyrighted sources and installation of any copyrighted software for which Shebbear College does not have an active license or explicit permission of the copyright owner, is strictly prohibited.
- Authoring or sending any form of electronic communications or messages, including, but not limited to, messages and emails that were unsolicited and may be considered junk mail, "chain letters", "Ponzi", hoax warnings or advertising, and that do not correctly identify you as the sender, or messages which appear to originate from another person.
- Unauthorised transmission, distribution, discussion or disclosure of information gained through a user's presence within Shebbear College or through the use of ICT facilities.
- Connecting any non-approved ICT device, system or service (including wireless access points) to Shebbear College's networks or setting up any network services, without the explicit or delegated permission from Authorised Personnel.
- Unauthorised access (or attempted unauthorised access) to any ICT facilities provided by Shebbear College.
- Allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the ICT facilities.
- Causing any damage to ICT facilities, including through the consumption of food or drink, or moving or removing such facilities without authorisation. Shebbear College reserves the right to charge for any damage caused.
- Attempting to modify, alter or in any way interfere with ICT facility security controls, hardware or software, configurations, settings, equipment, data files or websites without the written authorisation or delegated permission from Authorised Personnel.
- Introduction of unauthorised and/or malicious software or programs into the ICT facilities, including, but not limited to: unlicensed software, viruses, worms, Trojan horses or logic bombs; by downloading, creating or using any program, tool or item of software designed to

monitor damage, disrupt or interfere with the functioning of ICT facilities, user accounts or data.

- Effecting security breaches or disruptions of network communication, including, but not limited to, accessing or modifying data (or data headers) of which the user is not an intended recipient or logging into an ICT system or service, or account, that the user is not expressly authorised to access. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
- Executing any form of network monitoring including any data capture, port scanning or security scanning without written authorisation or delegated permission from Authorised Personnel.
- Registering for any system or service, including, but not limited to, social media accounts, web applications, domain names, which includes the name of Shebbear College or any similar name, or abbreviation that may mislead the public into believing that the domain name refers to Shebbear College.
- Acting in any way that directly or indirectly causes disruption to others' use of Shebbear College ICT facilities or using ICT facilities to disrupt or deny the use of ICT facilities of third parties at any time.

Remote Access

- Remote access to Shebbear College network is possible where this has been granted by the ICT Department.
- Remote connections are considered direct connections to Shebbear College network. As such, generally accessing services remotely subjects the user to the same conditions, requirements and responsibilities of this policy.

Social Media

- As a College we recognise that social media and networking are playing an increasing role within everyday life and that many staff are users of tools such as Facebook and Instagram for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. Staff should apply the guidance given in Social Media policies with regard to social networking.