E Safety Policy

Crisp Vocational Provision Ltd

Building futures for tomorrow

Approved by:	Emma Williams	**Date: September 2025**
Last reviewed on:	November 2026	
Next review due by:	September 2027	

Contents

Statement of Intent 2
Aims 2
Responsibilities..... 3
Headteacher and senior leaders 3
Proprietor 3
Designated Safety Lead (DSL)..... 4
Online Safety Lead 5
Tutors 5
IT Provider 6
Students 7
Parents and carers 7
Reporting and responding 8
School actions 9
Filtering and Monitoring 10
Filtering 10
Monitoring 10
Technical Security 11
Mobile Devices 12
School owned/provided devices 12
Personal devices: 12
Related Policies 12

Statement of Intent

This E-Safety Policy applies to all members of the Crisp Vocational Provision community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of

provision digital systems, both in and out of the provision. It also applies to the use of personal digital technology on the provision site.

Crisp Vocational Provision will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Aims

The aim of this E-Safety Policy is to ensure that all students, staff, and stakeholders within our Provision setting are equipped with the knowledge, skills, and support to use digital technologies safely, responsibly, and respectfully. We recognise that our students may face increased vulnerabilities and risks online, and we are committed to creating a secure digital environment that promotes wellbeing, inclusion, and safeguarding.

Our specific aims are to:

- Protect learners from online harm, including cyberbullying, exploitation, radicalisation, and exposure to inappropriate content.
- Promote responsible digital citizenship, encouraging respectful communication, critical thinking, and ethical online behaviour.
- Support learners with tailored guidance, recognising their individual needs and experiences, and providing accessible, age-appropriate education on e-safety.
- Empower staff and carers with the tools and training needed to identify, respond to, and prevent esafety concerns.
- Ensure safe use of school technology and networks, with clear protocols for monitoring, filtering, and reporting misuse.
- Foster a culture of openness and trust, where learners feel confident to speak up about online issues and seek help without fear of judgement.

This policy forms part of our wider safeguarding framework and reflects our commitment to nurturing a safe, supportive, and digitally aware learning environment.

Responsibilities

To ensure the online safeguarding of members of our provision it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the provision.

Headteacher and senior leaders

•The headteacher has a duty of care for ensuring the safety (including online safety) of members of the provision community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

•The headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff .

•The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

•The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

•The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.

•The headteacher/senior leaders will work with the proprietor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Proprietor

The DfE guidance "Keeping Children Safe in Education" states:

"Proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

This review will be carried out by the management team whose members will receive regular information about online safety incidents and monitoring reports. A member of the management team will take on the role of Online Safety Officer to include:

•regular meetings with the Designated Safeguarding Lead / Online Safety Lead

•regularly receiving (collated and anonymised) reports of online safety incidents

•checking that provision outlined in the Online Safety Policy

•Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider) - in-line with the DfE Filtering and Monitoring Standards

•reporting to relevant governors group/meeting

•Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen The DSL will:

•hold the lead responsibility for online safety, within their safeguarding role.

•Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online

•meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out

•attend relevant governing body meetings/groups

•report regularly to headteacher/senior leadership team

•be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.

•liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

The school will need to decide whether to appoint an Online Safety Lead to support the DSL. If the DSL & OSL roles are combined the following should be added to the DSL role above.

Online Safety Lead

The Online Safety Lead will:

•lead the Online Safety Group

•work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), (where these roles are not combined)

•receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments

•have a leading role in establishing and reviewing the school online safety policies/documents

•promote an awareness of and commitment to online safety education / awareness raising across the school and beyond

•liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated

•ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

•provide (or identify sources of) training and advice for staff/governors/parents/carers/learners •liaise with PowerUpIT

•receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education: •
content

- contact
- conduct
- commerce

Tutors

Tutors will work with the DSL/OSL to develop a planned and coordinated online safety education programme,

This will be provided (amend/delete as relevant) through:

•a discrete programme

•PHSE and SRE programmes

•A mapped cross-curricular programme

•assemblies and pastoral programmes

•through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

•they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices

•they understand that online safety is a core part of safeguarding

•they have read, understood, and signed the staff acceptable use agreement (AUA)

•they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations

•all digital communications with students, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use provision-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements

•they immediately report any suspected misuse or problem to (insert relevant person) for investigation/action, in line with the school safeguarding procedures

•online safety issues are embedded in all aspects of the curriculum and other activities

•ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

•they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices

•in lessons where internet use is pre-planned learners are 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

•there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc

•they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

•they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity

•they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies

•they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

IT Provider

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

- procure systems

- identify risk
- carry out reviews
- carry out checks

The IT Provider is responsible for ensuring that:

•they are aware of and follow the Crisp Vocational Provision Online Safety Policy and Technical Security Policy to carry out their work effectively in line with provision policy

•the Crisp Vocational Provision technical infrastructure is secure and is not open to misuse or malicious attack

•the provision meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body

•there is clear, safe, and managed control of user access to networks and devices

•they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

•the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) for investigation and action

•the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

•monitoring systems are implemented and regularly updated as agreed in school policies

Students

•are responsible for using the provision digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy

•should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

•should know what to do if they or someone they know feels vulnerable when using online technology.

•should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

•should understand the importance of adopting good online safety practice when using digital technologies out of provision and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

Crisp Vocational Provision will take every opportunity to help parents and carers understand these issues through:

•publishing the school Online Safety Policy on the school website

•providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)

•publish information about appropriate use of social media relating to posts concerning the school.

•seeking their permissions concerning digital images, cloud services etc

•parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the provision in:

•reinforcing the online safety messages provided to learners in provision.

•the handing in of devices in line with the Behaviour expectations

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"

Crisp Vocational Provision will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of the provision which will need intervention. The provision will ensure:

•there are clear reporting routes which are understood and followed by all members of the provision community which are consistent with the provision safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

•all members of the school community will be made aware of the need to report online safety issues/incidents

•reports will be dealt with as soon as is practically possible once they are received

•the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.

•if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include

- Non-consensual images
- Self-generated images
- Terrorism/extremism
- Hate crime/ Abuse
- Fraud and extortion
- Harassment/stalking
- Child Sexual Abuse Material (CSAM)
- Child Sexual Exploitation Grooming
- Extreme Pornography
- Sale of illegal materials/substances
- Cyber or hacking offences under the Computer Misuse Act • Copyright theft or piracy

•any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the proprietor

•where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss

•where there is no suspected illegal activity, devices may be checked using the following procedures:

•one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.

•conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.

•ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

•record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form

•once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- internal response or discipline procedures
- involvement by local authority / MAT (as relevant)
- police involvement and/or action

•it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively

•there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident

•incidents should be logged using Arbor or CPOMs as appropriate.

•relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.

•those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions

•learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:

•the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with

•staff, through regular briefings

•learners, through assemblies/lessons

•parents/carers, through newsletters, school social media, website

•the proprietor, through regular safeguarding updates

•local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures.

Filtering and Monitoring

The provision filtering and monitoring provision (Senso) is regularly reviewed at least annually and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility the filtering and monitoring provision is reviewed by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider (PowerUpIT). Checks on the filtering and monitoring system are carried out by a senior leader, the Designated Safeguarding Lead, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced.

Filtering

•the provision manages access to content across its systems for all users and on all devices using the CVP internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

•illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated

•there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures

•there is a clear process in place to deal with, and log, requests/approvals for filtering changes

•filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

•There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Headteacher are involved in the process and aware of the findings.

•Devices that are provided by the school have school-based filtering applied irrespective of their location.

Monitoring

Crisp Vocational Provision has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users:

•The provision monitors all network use across all its devices and services.

•monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.

•There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

•Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

•The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.

•Devices that are provided by the provision have monitoring applied irrespective of their location.

•monitoring enables alerts to be matched to users and devices.

Technical Security

The provision technical systems will be managed in ways that ensure that the provision meets recommended standards in the DfE Technical Standards for Schools and Colleges:

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- A documented access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually. All users (staff and students) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- password policy and procedures are implemented and are consistent with guidance from the National Cyber Security Centre
- all school networks, devices and system will be protected by secure passwords
- the administrator passwords for school systems are kept in a secure place
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (airgapped) copies off-site or in the cloud,
- PowerUP IT is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile.
- systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- dual-factor authentication is used for sensitive data or access outside of a trusted network
- where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.

- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

Mobile Devices

School owned/provided devices:

•all provision devices are managed though the use of Mobile Device Management software

•the asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed

•any designated mobile-free zone is clearly signposted

•personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are wellcommunicated.

•the use of devices on trips/events away from school is clearly defined and expectation are wellcommunicated.

•liability for damage aligns with current school policy for the replacement of equipment.

•education is in place to support responsible use.

Personal devices:

•where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.

•where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storge is be made available.

•use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems

•taking/storing/using images/video on personal devices is not permitted. The non-consensual taking/using of images of others is not permitted.

•liability for loss/damage or malfunction of personal devices is stated in the acceptable use policy

•at the point of entry for visitors provision expectations and requirements around mobile technology is communicated

•education about the safe and responsible use of mobile devices is included in the provision online safety education programmes

Related Policies

- Safeguarding policy
- Whistleblowing policy
- Behaviour policy
- Anti-bullying policy
- Artificial Intelligence Policy

- Acceptable Use Agreements

- Curriculum Policy
- Staff Handbook
- Safeguarding Handbook