Nacro Education
Online Safety Policy

Title: Online Safety Policy		**Version 2.**	
Authorised by	Education Safeguarding Leadership Group	**Date Authorised**	30.05.24
Annual Review	August 2026	**Next Full Review Date**	August 2027

Contents

1. Policy Statement 2
2. Scope of the Online Safety Policy 2
3. Related policies 3
4. Relevant Legislation and Guidance 3
5. Aims 4
6. Roles and Responsibilities 5
7. Safeguarding 9
8. Acceptable Use 12
9. Reporting and Responding 12
10. Online Safety Education and Awareness 15
11. Filtering & Monitoring 16
12. Social Media 19

APPENDICES 21

1. Policy Statement

The internet and digital technologies provide significant opportunities for learning, communication, personal development and participation in modern society. However, they also present risks, including cyberbullying, online sexual harassment, exploitation, grooming, radicalisation, misinformation and disinformation, privacy breaches, sharing of nudes and semi-nudes, harmful online content, and AI-facilitated harms such as impersonation and deepfakes. These risks can have significant impacts on personal safety, mental and physical wellbeing and healthy relationships. Digital technologies also present cyber security risks that may affect the confidentiality, integrity and availability of Nacro systems and information.

Nacro therefore makes all efforts, including technical and educational, to help create a safe yet flexible environment for using such technology across its education provision, recognising that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all students and staff are protected from potential online harm.

Nacro understands that all students should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

Use of Artificial Intelligence (AI)

Nacro recognises that Artificial Intelligence (AI), including generative AI technologies, is becoming increasingly accessible to students and staff. Whilst AI can support learning and productivity, it may also create safeguarding, privacy, misinformation and cyber security risks.

Nacro will:

- promote responsible and safe use of AI technologies;
- educate students and staff regarding AI-related risks;
- consider AI-related risks within safeguarding and online safety risk assessments;
- ensure the use of AI does not compromise safeguarding, confidentiality or data protection obligations;
- monitor emerging developments in AI and review practice accordingly.

Nacro maintains a zero-tolerance approach to any forms of abuse including bullying, whether online and/or in person, sexual harassment, and violence, racist, sexist, and homophobic (or any other trans-related phobias) behaviour and abuse. Students and staff are encouraged to report any concerns or issues, however small, to a trusted member of staff and/or the Centre Designated Safeguarding Lead (DSL) so that appropriate and timely action can be taken, and relevant support offered. The Designated Safeguarding Lead for Education will always be informed of concerns raised through Nacro's internal alert system.

This policy has been developed by

- Nacro's Head of Performance and Assurance
- Designated Safeguarding Lead for Education.

This policy considers guidance issued by the UK Safer Internet Centre and NSPCC Learning and should be read in conjunction with Nacro's Child Protection and Safeguarding Policy and Procedures

and related safeguarding policies, as well as the Learner Declaration form (a template of which can be found in Appendix 2), that is completed as part each learner's assessment process.

2. Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Nacro to safeguard our students and staff in accordance with statutory guidance and best practice.

This policy relates to the use of digital technology and online services including:

- internet access and web-based services;
- email and messaging systems;
- virtual learning environments;
- cloud-based platforms and storage systems;
- social media platforms;
- video conferencing and live-streaming platforms;
- mobile phones, tablets, laptops and wearable technology;
- digital photography, audio and video recording technologies;
- personal devices used on Nacro premises or networks;
- AI and generative AI tools;
- emerging technologies and digital services.

This policy applies regardless of whether access is obtained through Nacro equipment, personal devices, Nacro networks, student Wi-Fi, home internet connections or approved third-party learning technologies

This Online Safety Policy applies to all staff, students, trustees, volunteers, parents and carers, visitors, who have access to and are users of Nacro's student Wi-Fi facilities. This policy relates to the misuse of the above technologies, which affects the safety and welfare of others or where the culture, values, or reputation of Nacro are put at risk.

The Education and Inspections Act 2006 empowers the CEO, to such an extent as is reasonable, to regulate the behaviour of students when they are off Nacro premises and empowers Nacro employees to impose disciplinary sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of, but is linked to membership of the Nacro. Nacro will deal with such incidents within this policy and related policies and will, where known, inform parents/carers and/or external agencies of incidents of inappropriate e-safety behaviour that takes place outside of Nacro.

3. Related policies

- Child Protection and Safeguarding Policy and Procedures
- Anti-bullying Policy
- Positive Engagement and Behaviour Policy and Procedures.
- Data Protection Policy
- Health and Safety Policy
- Prevent Policy
- Staff Code of Conduct

4. Relevant Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for colleges on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. Further applicable legislation and guidance which informs this policy can be found below:

- Online Safety Act 2023
- Working Together to Safeguard Children 2023
- DfE The Prevent Duty
- Counter Terrorism and Securities Act 2015
- UK Safer Internet Centre Guidance
- DfE Meeting Digital and Technology Standards in Schools and Colleges.
- DfE Filtering and Monitoring Standards
- DfE guidance relating to Generative Artificial Intelligence

National Cyber Security Centre (NCSC) Cyber Security Standards for Schools and Colleges
UK Council for Internet Safety (UKCIS) guidance on Sharing Nudes and Semi-Nudes
Nacro will regularly review emerging guidance relating to online safety, cyber security and artificial intelligence.

This policy also reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

5. Aims

Nacro aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers, and Trustees.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Nacro Education community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

And through this policy:

- Identify roles and responsibilities relating to online safety at Nacro.
- Safeguard and promote the welfare of students by minimising and mitigating against cyberbullying and other forms of abuse.
- Encourage students to make good use of the educational and personal development opportunities presented by access to the internet and other electronic communication.
- Minimise the risk of harm to assets and reputation of Nacro.
- Help students and staff take responsibility for their own online safety.
- Ensure students and staff use technology safely and securely.
- Educate students and staff about potential threats and harms arising from internet use.
- Maintain robust systems for web filtering and monitoring.

The liability of Nacro
Unless negligent under the terms of this policy, Nacro accepts no responsibility to the student, parents or carers caused by or arising out of a student's use of mobile phones, email, and the internet whilst at Nacro.

Take down policy.
Should Nacro become aware that any resource, image, or media have been uploaded which the College does not have the copyright permission to use, it will be removed as soon as possible.

Digital recording

Audio recordings, photographs, screenshots, screen recordings and video recordings involving students, staff or visitors must only be created where there is a legitimate educational, operational or safeguarding reason and all appropriate permissions have been obtained.
Unauthorised recording, image capture, screen capture, sharing or distribution of digital content relating to any member of the Nacro community may result in disciplinary action and/or safeguarding intervention.

Monitoring and review
Online safety incidents must be recorded and will be logged on to Nacro's Information Management System which will create an alert to the appropriate levels of authority depending on the nature of concern. The Designated Safeguarding Lead is alerted through the system in the event of all Safeguarding related incidents.

The Head of Performance and Assurance, along with the Designated Safeguarding Lead for Education has responsibility for the implementation and annual review of this policy in consultation with staff, students, parents/carers and may consult with external specialist individuals or agencies to support this.

The Designated Safeguarding Lead for Education will consider the record of online safety incidents, new or emerging threats or risks and new technologies and will also consider if existing security procedures are adequate and fit for purpose.

Annual Online Safety Risk Assessment

The Designated Safeguarding Lead will coordinate an annual online safety risk assessment considering:

- student vulnerability and safeguarding needs;
- SEND and additional vulnerabilities;
- local and contextual safeguarding risks;
- online safety incident trends;
- effectiveness of filtering and monitoring arrangements;
- cyber security risks;
- risks arising from artificial intelligence and emerging technologies;
- staff training requirements.

Actions arising from the assessment will be documented, monitored and reported through appropriate governance arrangements

6. Roles and Responsibilities

To ensure the online safeguarding of members of Nacro's Education community it is important that we all 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 Nacro.

Nacro Board of Trustees/Education Committee

The board of Trustees has overall responsibility for the approval and monitoring of this policy and holding Nacro's Principal for Education to account for its implementation.
The board of Trustees will co-ordinate regular meetings with appropriate staff to discuss online safety, and scrutinise information provided by the designated safeguarding lead (DSL).
All Trustees will:

- Ensure they have read and understand this policy.
- Adhere to Nacro's Guidance for users on acceptable behaviours regarding online safety (which can be found in Appendix 1 of this policy).

Education Committee

Responsible for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body"

The Education Committee will receive assurance regarding:

- outcomes of the annual online safety risk assessment;
- online safety incident trends;
- effectiveness of filtering and monitoring arrangements;
- cyber security risks impacting education provision;
- safeguarding implications of emerging technologies and AI

Education Committee members will receive regular information about online safety incidents and monitoring reports. A member of the Committee will take on the role of Online Safety Lead to include:

- Regular meetings with the Designated Safeguarding Lead
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Checking that provision outlined in the Online Safety Policy is taking place (e.g., online safety education provision and staff training is completed as intended)
- 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 and involve the responsible governor), in-line with the DfE Filtering and Monitoring Standards.

Director (Principal) for Education

- The Principal has a duty of care for ensuring the safety (including online safety) of members of Nacro's Education 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 Principal and (at least) another member of the senior leadership team 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 Principal is 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 conduct their roles and train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those who carry out the internal online safety monitoring role.
- The Principal will receive regular monitoring reports from the Designated Safeguarding Lead.
- The Principal will collaborate with the responsible Trustee, the designated safeguarding lead

(DSL) and IT service providers in all aspects of filtering and monitoring.

Designated Safety Lead (DSL)

The DSL will:

- Support the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the education centres.
- Receive relevant and regularly updated training/guidance 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 Principal, Head of ICT, Head of Performance and Assurance and other staff to discuss current issues, review (anonymised) incidents and filtering and monitoring logs, ensuring (at least) annual filtering and monitoring checks are carried out.
- Attend relevant governing body meetings/groups - Education committee specifically.
- Report regularly to Education Committee and Senior leadership team.
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with Nacro's Positive Engagement and Behaviour policy.
- 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).
- Liaise with other agencies and external staff if necessary.

Teaching and Support Staff

Nacro staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and Nacro's Online Safety Policy and procedures.
- they understand that online safety is a core part of safeguarding.
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem for investigation/action, in line with safeguarding reporting procedures.
- all digital communications with students and parents/carers are on a professional level and only carried out using official systems.
- maintain appropriate professional boundaries online;
- communicate with students only through approved Nacro systems and platforms;
- not communicate with students through personal social media accounts, messaging services or personal email accounts;
- ensure that AI tools are not used in ways that compromise confidentiality, safeguarding or data protection requirements;
- report any inappropriate online contact or communication involving students.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure students 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 activities (where allowed) and implement current policies regarding these devices.

- In lessons where internet use is pre-planned students 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
- Where lessons take place using live-streaming or videoconferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- 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 outside of Nacro and in their use of social media.

ICT Provision

Nacro's ICT Provision (including outsourced ICT providers) are responsible for ensuring that:

- They are aware of and follow Nacro's Online Safety Policy to carry out their work effectively in line with Nacro policies.
- Nacro's technical infrastructure is secure and is not open to misuse or malicious attack.
- Nacro meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority 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 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 DSL for investigation and action.
- Ensure that web filtering and monitoring is implemented and working effectively to implement the requirements of Nacro's Online Safety Policy and Information Security Policies.

Students

- Are responsible for using Nacro's digital technology systems in accordance with the student 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 understand the importance of adopting good online safety practice when using digital technologies outside of Nacro and realise that Nacro's Online Safety Policy covers their actions outside of Nacro, if related to being a Nacro student.

Students are also expected to:

- use strong passwords and keep them secure;
- report suspicious online communications, phishing attempts or cyber security concerns;
- avoid downloading unauthorised software;
- use digital technologies responsibly and safely;

follow Nacro guidance regarding cyber security and acceptable use

Parents and Carers

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

Nacro will take every opportunity to help parents and carers understand these issues through:

- Publishing Nacro's Online Safety Policy on its website
- Inclusion within the Student Handbook
- Publish information about appropriate use of social media relating to posts concerning Nacro.
- Seeking their permissions concerning digital images, cloud services etc where under 18
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.
- Nacro will, where appropriate, provide information and guidance to parents and carers regarding:
    - social media trends;
    - cyber security;
    - misinformation and disinformation;
    - online exploitation;
    - artificial intelligence tools;
    - emerging online safeguarding risks.
    -

Parents and carers will be encouraged to support Nacro in:

- Reinforcing the online safety messages provided to students.
- The safe and responsible use of their children's personal devices in Nacro (where this is allowed)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and Members of the Community

Visitors and members of the community who use Nacro's ICT systems or internet will be made aware of this policy, when relevant, as well as the visitors information sheet which includes detail regarding online safety. All visitors are required to read and accept the visitor's information sheet.

7. Safeguarding

While technology can facilitate a world of learning and development in addition to creating opportunities, the stark reality is that it can also lead to potential and actual harm and abuse. It can elicit and support a wide range of illegal abusive behaviours. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk, otherwise called the 4 Cs:

- **Content:** Being exposed to illegal, inappropriate or harmful content, including pornography, misinformation, disinformation, conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, deepfakes and harmful AI-generated content.

Contact: Being subjected to harmful online interaction with other users, e.g., peer-to-peer pressure, commercial advertising, and adults posing as children/young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct**: Online behaviour that increases the likelihood of, or causes, harm, including cyberbullying, online sexual harassment, discriminatory abuse, sharing nudes and semi-nudes, online exploitation, impersonation and misuse of AI-generated content.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Hidden harms: Types of online abuse may include, but are not limited to:

Type	**Example**
Cyberbullying	Sending harmful text messages, via social media, spreading rumours online, circulating false information, posting, or sharing private images, impersonating someone online.
Harassment/Stalking	Bullying, Cyber stalking, Antisocial behaviour, Sexual Harassment, Stalking, Online stalking, and harassment
Threatening behaviour	Direct or Indirect threats of violence, throwing objects, Challenges to fight, Shoving, Physical Attacks, Threatening phone calls, Emails, or Other Correspondence
Emotional abuse	Verbal Abuse, Public Embarrassment, Dismissiveness, Isolation, Threats to Violence
Grooming	Grooming is a process where an offender builds a relationship with a young person, gaining their trust and a position of power over them in preparation for abuse. Signs of grooming include, asking a young person to keep a secret, information gathering, sending sexual messages or images, giving gifts or special attention or threats of violence.
Sharing Nudes and Semi-Nudes	Creating, receiving, possessing, requesting or sharing nude or semi-nude images, videos or messages, including manipulated or AI-generated imagery.

Sexual abuse/exploitation, and harassment.	Includes trafficking and prostitution, threatened physical intrusion of aa sexual nature whether by force or under unequal or
AI related harm	Creation, sharing or use of deepfakes, AI-generated imagery, impersonation, manipulated media, misinformation, extortion, harassment or exploitation facilitated through artificial intelligence technologies.
	coercive conditions. Includes sexual slavery, pornography, child abuse and sexual assault.
Upskirting	'Upskirting' is an informal term for a type of voyeurism when someone uses equipment like a camera or mobile phone to take photos or videos underneath a person's clothes, without their permission
Criminal exploitation	Criminal exploitation is often a feature of, but not limited to, 'county lines' drug dealing. Victims can be coerced or groomed into committing crime through debts, violence, or manipulation. They can be made to hold or store weapons, engage in theft and shoplifting, money laundering and even begging.
Radicalisation/Extremism	Radicalisation is defined as the process by which people come to support terrorism and extremism and, in some cases, to then participate in terrorist groups.
Blackmail/Extortion	Blackmailers usually want money in return for keeping something secret. Anyone making threats and demands in return for keeping a secret is engaged in blackmail e.g., sending nude/inappropriate pictures, to extort money
Hate Crime	A hate crime is crime where a perpetrator targets a victim because of their physical appearance or perceived membership of a certain social group. Types of hate crime include physical assault, verbal abuse, and incitement to hatred.

Sharing of inappropriate/illegal material.	Inappropriate content may include sexually explicit material •false or misleading information • violence • extremism or terrorism • hateful or offensive material. The exposure of young people to inappropriate content is difficult to measure because many instances go unreported.

Other factors to consider include:

- Recognising that students behave differently online as they feel protected with anonymity and invisibility. This can cause them to take risks where they perhaps wouldn't otherwise outside of the online platforms.
- Understanding that students can often pass off unacceptable or harmful online behaviours as so-called social norms or just banter. For example, language that can be used, and in some cases is often expected, as part of online gaming and the normalisation of misogynistic, homophobic, and racist language that would not be tolerated offline.

8. Acceptable Use

This Online Safety Policy and Learner Acceptable Use Declaration (Appendix 2) define acceptable use at Nacro. The acceptable use declaration in Appendix 2 of this policy will be communicated/re-enforced through:

- Student handbook and induction
- Staff induction
- Communication with parents/carers
- Embedded within the curriculum.
- Nacro website.

9. Reporting and Responding

Online safety concerns

Online safety concerns may fall under three core areas:

1. **Safeguarding** for example cyberbullying, online grooming, online sexual harassment, misogynistic abuse, discriminatory abuse, harmful online trends or challenges, sharing nudes and semi-nudes, deepfake content, AI-generated harmful content, impersonation and online exploitation.
2. **Discipline** for example, abusive or inappropriate communication between staff.
3. **Cybersecurity** for example external email hacking.

These are not mutually exclusive, so concerns may fall under one or all areas in certain circumstances.

Every online safety concern will be assessed in relation to safeguarding, discipline and cybersecurity risk, Typically, however concerns will be dealt with in the following way:

- **Safeguarding Issues** will be managed in accordance with Nacro's Safeguarding Policies and Procedures.

- **Student discipline issues** that are not safeguarding related will be dealt with in accordance with the Positive Behaviour and Engage Policy and Procedures.
- **Staff discipline issues** will be dealt with through Nacro's HR policies and procedures and in accordance with the Employee Code of Conduct.
- **Filtering and monitoring online use** will be dealt with by the Head of Performance and Assurance and Head of ICT in conjunction with the Designated Safeguarding Lead.
- **Cybersecurity issues** will be dealt with by the Head of Performance and Assurance and Head of ICT.

Nacro will take all reasonable precautions to ensure online safety for all students but recognises that incidents may occur inside and outside of Nacro which will need intervention. Nacro will ensure there are clear reporting routes which are understood and followed by all members of Nacro's Education community which are consistent with the safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

All members of the 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 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 Nacro's 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
- Upskirting
- 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 Designated Safeguarding Lead, unless the concern involves the DSL, in which case the complaint is referred to the Principal.

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 students 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 e.g., LADO
    - 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, employee assistance programme, for those reporting or affected by an online safety incident.
- incidents should be logged on Nacro's incident management system.
- 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 National Safeguarding Board, Health, and Safety Committee and/or Security Working Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with staff, through regular briefings.
    - students, through lessons and student forums
    - parents/carers, through newsletters, social media, website
    - trustees, 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"*

It is important that any incidents relating to students or staff are dealt with as soon as possible in a proportionate manner and in line with Nacro's safeguarding policies and the Positive Engagement and Behaviour policy and procedures.

10. Online Safety Education and Awareness

Online Safety Education Programme

To ensure staff can respond appropriately, Nacro will:

- Ensure provision of policies and practices as part of induction and ongoing training provision.
- Provide up to date online safety training at least annually or more, in line with legislative and statutory changes and/or online safety incidents arising.
- Inform staff and learners of monitoring and filtering processes.

- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.
- Advise of appropriate resources.
- Add mandatory online safety to NacroLearn.
- The Head of Assurance and Performance and the DSL will complete regular horizon scanning of legislative changes, updated guidance, and trends to keep up to date with regulatory changes/emerging trends.

Staff training will also include:

- filtering and monitoring responsibilities;
- cyber security awareness;
- misinformation and disinformation;
- online sexual harassment;
- sharing nudes and semi-nudes;
- generative AI and related safeguarding risks;
- reporting routes and escalation procedures.

Educating Students about Online Safety

To ensure students are safe and responsible online, Nacro will:

- Educate students regarding safe and responsible use and access of the internet.
- Include online safety as mandatory within all tutorial sessions (including employability, enrichment, and pastoral sessions).
- Reinforce online safety messages during curriculum delivery.
- Include annual mandatory online safety training for staff.

Students will be taught about online safety as part of the curriculum and will learn to:

- use technology safely, respectfully, responsibly and securely, including protecting their online identity, privacy and personal information;
- recognise inappropriate, harmful or illegal content, contact and conduct online, and understand how to respond appropriately;
- understand how technological developments, including social media, algorithms, generative artificial intelligence (AI) and emerging technologies, can impact online safety and wellbeing;
- identify misinformation, disinformation and conspiracy theories, and evaluate the reliability of online information;
- understand cyber security basics, including the importance of strong passwords, multi-factor authentication, phishing awareness and safe use of online services;
- recognise the risks associated with online relationships, online sexual harassment, exploitation, bullying and discriminatory behaviour;
- understand the risks associated with sharing nudes and semi-nudes and other harmful online behaviours;
- know how, when and where to seek help and report online safety concerns, both within Nacro and externally where appropriate.

The safe use of social media and the internet will also be covered in other subjects where relevant. Nacro will use lessons, tutorials, Student Voice forums to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

Educating Parents / Carers about Online Safety

Nacro will raise parents' / carers' awareness of internet safety in letters, newsletters or other within communications home, and in information published via our website including any topical issues that may arise with advice and guidance should there be a need.

This policy will also be available to parents/carer's via Nacro's website. Online safety will also be covered during parent / carer evenings and information events.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal, DSL add details and or by emailing safeguarding@nacro.org.uk. Concerns or queries about this policy can be raised as above.

11. Filtering & Monitoring

Nacro maintains a robust system for filtering and monitoring online use, in compliance with DfE statutory guidance 'Filtering and Monitoring Standards for Schools and Colleges,' and 'Keeping Children Safe In Education (KCSIE).' The aim of this is to block harmful and inappropriate content without unreasonably impacting teaching and learning, as well as ensuring data security.

It is important to note that while Nacro has systems in place these should not replace effective digital citizenship education though which an environment is created where all members of the Nacro community understand what appropriate online behaviour is and know how to protect themselves.

The Designated Safeguarding Lead (DSL) takes responsibility for safeguarding and online safety at Nacro. This includes overseeing and acting on web filtering and monitoring, safeguarding concerns and checks to filtering and monitoring systems.

Monitoring Alerts and Safeguarding Escalation

Potential safeguarding concerns identified through filtering or monitoring systems will be reviewed and escalated in accordance with safeguarding procedures.

The DSL, ICT colleagues and senior leaders will review alerts, patterns and trends to identify emerging safeguarding concerns, cyber security risks, misuse of systems and further training requirements

The DSL works closely with other senior staff members including Head of ICT who is responsible for technical maintenance and integrity of Nacro's ICT systems.

Staff devices have Windows Security and Microsoft Defender installed as standard, which is controlled by Nacro's IT administrative team, providing an additional layer of protection against potentially harmful files.

Blocking and Filtering Harmful and Inappropriate Content

At Totton College, Nacro deploys WatchGuard as a filtering and monitoring system, to filter and monitor harmful and inappropriate content. Nacro's filtering and monitoring system at Education Centres is managed and maintained by BT.

Nacro's filtering systems are configured to restrict access to harmful, illegal and inappropriate content including:

- sexually explicit content;
- extremist and terrorist material;
- hate content;
- self-harm and suicide content;
- illegal drugs;
- criminal activity and hacking tools;
- violence and weapons;
- fraudulent, phishing and scam websites;
- other content identified through risk assessment processes.

Specific filtering categories may vary according to system provider arrangements and technological developments

Effective monitoring strategies

Nacro employs comprehensive monitoring strategies, which include network monitoring by Nacro's ICT Team, and physical monitoring by staff of user screens. This ensures prompt identification, appropriate consultation with other members of staff (including the senior leadership team and DSL) and resolution of potential issues, to provide a secure and safe online experience for all users.

Review of filtering and monitoring provision

Nacro will review filtering and monitoring arrangements:

- at least annually;
- following significant safeguarding incidents;
- following significant technological changes;
- where there are significant changes to the student cohort, identified risks or systems.

Reviews will involve the DSL, senior leaders and ICT colleagues.
Outcomes, actions, responsible owners and review dates will be formally documented

12. Social Media

Use of Nacro's social media channels

Nacro's social media posts may include:

- Announcements such as student's achievements, organisation events and updates.
- Student recruitment campaigns
- Media releases
- Marketing campaigns

Nacro does not automatically follow back everyone using its social media. Being followed, using hashtags and mentions of social media accounts does not imply endorsement from Nacro.

Nacro welcomes feedback and will try to respond to comments where possible and where right to do so. However, Nacro may not be able to reply individually to all messages received.

The use of 'like,' 'share' or comment on one of Nacro's posts will be publicly visible. Nacro may use contact information and/or usernames to respond to messages or comments received.

Publicly made posts on Nacro's social media may be shared with and/or re-published for Nacro followers. Usernames of followers are publicly available on our social media channels.

Nacro may also receive information from third parties, such as other social media users, if a user is mentioned, tagged or photo shared. Nacro may tag or share photos or content when uploading social media platforms. Users may unsubscribe and / or unfollow at any stage.

Expected behaviour when using Nacro social media.

Nacro expects it social media users to offer the same courtesy it offers to them:

- All users must comply with the social media platforms' term of use.
- Users are responsible for any content posted, i.e., content the user chooses to share.
- On Facebook Nacro will remove, in whole or in part, or ignore posts that are considered inappropriate or private.

Nacro will remove, block, ban and if necessary, report users to the associated social media platforms, who violate acceptable norms with direct messages that:

- bully, harass or intimidate.
- are unlawful, libellous, defamatory, abusive, threatening, harmful, obscene, profane, or discriminatory.
- are deceptive or misleading.
- infringe or violate someone else's rights.
- violate the law or intellectual property rights.
- are spam (persistent negative and / or abusive posts in which the aim is to provoke a response.
- advertise products or services.
- are irrelevant, off topic, disruptive or repetitive.

Nacro will also remove or ban any users who:

- encourage others to post such messages.
- use offensive images as their profile picture.
- have an offensive username.

Artificial Intelligence and Manipulated Content

Users must not knowingly create, publish, share or promote:

- deepfake content;
- impersonation accounts;
- misleading AI-generated content;
- misinformation or disinformation;

- harmful online trends or challenges;
- content intended to bully, harass, exploit or deceive others.

Concerns relating to such content must be reported through safeguarding or incident reporting procedures

Staff Use of Social Media

Staff must ensure that personal social media activity does not:

- compromise professional boundaries;
- disclose confidential information;
- adversely affect Nacro's reputation;
- undermine confidence in their professional role;
- create actual or perceived safeguarding concerns.

APPENDICES

Appendix 1: Guidance for users on acceptable behaviours regarding online safety

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks,	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography. • Incitement to and threats of violence					X

proposals or comments that contain or relate to:	• Hate crime. • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering. N.B. Schools should refer to guidance about dealing sharing nudes and semi-nudes – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
Users shall not undertake activities that might be classed as cyber-crime under the	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)					X

Computer Misuse Act (1990)	• Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices. • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences					

	should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in Nacro policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination					
	Using Nacro systems to run a private business				X	
	Using systems, applications, websites, or other mechanisms that bypass the				X	

	filtering/monitoring or other safeguards employed by Nacro					
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X		
	Any other information which may be offensive to others or breaches the integrity of the ethos of Nacro or brings into disrepute				X	

Activities	Staff and other adults				Students			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission / awareness
Online gaming				X				X
Online shopping/commerce			X					X
File sharing		X						X
Social media		X				X		
Messaging/chat		X				X		
Entertainment streaming e.g., Netflix, Disney+			X					X
Use of video broadcasting, e.g., YouTube, Twitch, TikTok			X					X
Personal mobile phones may be brought into Nacro		X				X		

Use of mobile phones for learning at Nacro						X		
Use of mobile phones in social time at Nacro		X				X		
Taking photos on personal mobile phones/cameras	X							X
Taking photos or recording on Nacro devices for work related purposes.			X					
Use of other personal devices, e.g., tablets, gaming devices			X					X
Use of personal e-mail in Nacro, or on Nacro network/wi-fi		X						X
Use of Nacro e-mail for personal emails			X					X

Users must not:

- use VPNs, proxy services or anonymising browsers to bypass filtering and monitoring controls;
- use unauthorised artificial intelligence tools;
- create or share harmful AI-generated content;
- create deepfakes or impersonations;

- enter confidential Nacro, staff or student information into unauthorised AI platforms;
- use software intended to bypass filtering, monitoring or cyber security controls.

Appendix 2: Learner Acceptable Use Declaration

Learner Name		Education Centre:	

This document summarises the Information, Advice & Guidance that has been provided and is aligned with the detailed Learner Assessment Form which outlines the aspirations, expectations, and current abilities of the learner. The following areas have been covered:

- The entry requirements of the chosen learning programme
- The implications of the choice of the programme including course outline
- An assessment of the suitability of the chosen programme, including any credits or exemptions which may be appropriate.
- Financial support required by the learner (including 16-19 Bursary, Free Meals, Advanced Learner Loan Bursary etc.) - as appropriate to the funded programme.
- Health and Safety Policy Statement, Emergency Procedures including evacuation routes and assembly point, First Aid arrangements, Welfare facilities.
- Equality, Diversity & Inclusion
- Safeguarding Policy
- PREVENT
- Online Safety Awareness
- misinformation and disinformation;
- conspiracy theories;
- cyber security;
- online sexual harassment;
- sharing nudes and semi-nudes;
- artificial intelligence risks;
- reporting online safety concerns
- Privacy Notices & GDPR
- General rules and information including: - Signing in & out of building.
- Compliments and Complaints procedure

The Standard			
We Will		**You will**	
1	Make every lesson enjoyable and challenging	**1**	Take an active part in every lesson
2	Set work which reflects our high expectations	**2**	Take responsibility for your own learning and stretch yourself to do more than you think you can
3	Be prompt and well prepared	**3**	Attend all lessons promptly and be well prepared
4	Not cancel lessons without ensuring work is set	**4**	Explain unavoidable absence and ensure missed work is covered
5	Agree and monitor targets with you	**5**	Agree and monitor your own targets
6	Give you regular, timely feedback so that you know how to improve	**6**	Act on feedback
7	Promote employability skills of reliability, tenacity, and teamwork	**7**	Practice employability skills
8	Set work which helps prepare you for exams and assessments	**8**	Complete all course work that is set for you in a timely manner

9	Treat you with respect and help to make the learning environment a safe place for everyone	**9**	Treat others with respect and help to make the learning environment a safe place for everyone
10	Celebrate your achievements with you	**10**	Tale pride in your achievements

Learner Declaration:

1. Based upon the result of my assessment and the information, advice and guidance provided I am satisfied that a suitable programme of learning has been designed for me.
2. Having discussed my timetable and exam requirements, I am willing and able to participate fully.

Learner Online Safety Declaration

I understand that:

- My online activity may have safeguarding implications
- I must report safety concerns online to a member of staff
- Cyberbullying, online harassment and sharing nudes and semi-nudes may result in safeguarding and disciplinary action;
- I must use digital technology responsibly and in accordance with Nacro expectations

		Date:	

Staff member undertaking the interview

Signed:		Date:	

This is an auditable document and should be retained on file

Appendix 3: Process for reporting online safety incidents.

All online safety concerns must be reported through CPOMS in accordance with Nacro safeguarding procedures or in the case of concerns relating to Staff via IMS2.

Immediate safeguarding concerns must be reported verbally to the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead without delay and recorded on CPOMS as soon as possible.

Concerns relating to cyber security should also be reported through ICT reporting channels.

Reports relating to online safety, filtering and monitoring alerts, AI-related concerns, online harassment, exploitation, harmful content or inappropriate digital behaviour will be managed in accordance with safeguarding, behaviour and information security procedures as appropriate.