Irlam and Cadishead Academy
The best in everyone™
Part of United Learning

IRLAM & CADISHEAD ACADEMY

E-Safety Policy 2024

Document Owner	Assistant Head - Mrs C Jones
Last Review	January 2024
Next Review	September 2025
Approved By	Principal - Mr C Leader
Ratified On	

Online Safety (e-Safety) Policy

Contents

1. Creating an Online Safety Ethos

1.1. Aims and Policy Scope

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provide the platform that facilitates harm. The Education and Inspections Act 2006 empowers the Principal to such extent as it reasonable, to regulate the behaviour of students when they are off the Irlam and Cadishead Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. An effective approach to online safety empowers the Academy to protect and educate the whole academy or community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

- **content**: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views.
- **contact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

- Irlam and Cadishead Academy believes that online safety (e-safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- Irlam and Cadishead Academy identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
- Irlam and Cadishead Academy has a duty to provide the academy community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the academy's management functions. ICA also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.
- The purpose of Irlam and Cadishead Academy's online safety policy is to:

  - Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
  - Clearly identify the key principles expected of all members of the community with regard to the safe and responsible use of technology to ensure that ICA is a safe and secure environment.
  - Safeguard and protect all members of ICA Community online.
  - Raise awareness with all members of the ICA community regarding the potential risks as well as benefits of technology.
  - To enable all staff to work safely and responsibly to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the academy (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals who have been provided with academy issued devices for use off-site, such as a work laptop/ Surface Pro's or mobile phones.
- This policy must be read in conjunction with other relevant academy policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education (SRE).

1.2. Writing and Reviewing the Online Safety Policy

- Irlam and Cadishead Academy's online safety policy has been written by the academy, involving staff, students
  and parents/carers, building on the United Learning online safety policy template.
- The policy has been approved and agreed by the Leadership Team and governing body.
- The academy's Online Safety (e–Safety) Policy and its implementation will be reviewed at least annually or sooner if required.
- The school will monitor the impact of the policy using:
  - Logs of reported incidents
  - Monitoring logs of internet activity (including sites visited)/filtering.
    - Surveys/questionnaires of students, parents/carers/staff

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	{in draft format}
The implementation of this online safety policy will be monitored by:	Catherine Jones
Monitoring will take place at regular intervals:	Every September
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Every October
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	
Should serious online safety incidents take place, the following external persons/agencies should be informed as necessary:	LA Safeguarding Officer, Academy Group Officials, LADO, Police

1.3. Key Responsibilities of the Community

1.3.1. Key Responsibilities of the Leadership Team

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the academy community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the academy community and ensuring that the filtering and academy network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole academy curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the academy/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of academy systems and networks.

1.3.2. Key Responsibilities of the Online Safety/Designated Safeguarding Lead

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up to date with current research, legislation and trends. (Including National Cyber Security Centre-weekly threat report)
- Coordinating participation in local and national events to promote positive online behaviour, e.g., Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Working with the academy/setting lead for data protection and data security to ensure that practice is in line with legislation.
- Through CPOMS, maintaining an online safety incident/action log to record incidents and actions taken as part of the academy's safeguarding recording structures and mechanisms.
- Monitoring Internet filtering reports to identify behaviour which might indicate safeguarding issues or inappropriate behaviours. Update safeguarding log or e-safety incident log as appropriate.
- Monitoring the academy/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the academy leadership team, Governing Body and other agencies as appropriate.

- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate academy policies and procedures.

1.3.3. Key Responsibilities of Staff

- Contributing to the development of online safety policies.
- Reading and signing the academy Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of academy/setting systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.
- Software settings- ensuring staff check the settings for software intended to be used, for example platforms are not set to default and allow uses unfiltered access to inappropriate areas. This also includes the use of free software which can have adverts placed on the interface, these adverts could potentially distract the students. It is the Staff teacher's responsibility to personally check the links.
- Communication of the importance of secure passwords. Students are also aware that if they forget their passwords, their Form Tutor is their first port of call, who will reset their password for them.
- Students can access the student work area on the school website and access the learning platforms, the first row of boxes allows the students to reset passwords for the learning platforms, as well as how to access Knowledge Organisers, setting up and using Microsoft Teams.

1.3.4. Additional Responsibilities of Staff Managing the Technical Environment

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on academy-owned devices.
- Ensuring that the academy's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

- Checks on appropriate licences to allow staff and students to access the chosen learning platforms and software.
- Configure internet filters to generate regular safeguarding reports, as determined by e-safety lead, pastoral leads and DSL, and send to appropriate staff.
- Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the academy's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

Technical infrastructure/equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- ICA technical systems will be managed in ways that ensure that academy meets recommended technical requirements as set out in the Department for Education's "Meeting digital and technology standards in schools and colleges".
- ICT technicians run a weekly check- where they check for devices that have not reported back to Smoothwall monitor in the last few days and it is investigated (Salford regular proactive checks) This data is collated on Smoothwall.
- ICA has a 24/7 filtering system so any concerns are emailed straight away. Alerts are emailed directly to staff from Smoothwall. Smoothwall have a contract where they will check to see if the filtering system setup has not changed or been deactivated.
- There will be regular reviews* (at least annually or when: a safeguarding risk is identified, there is a change in working practice and/or new technology is introduced) and checks** of the safety and security of the academy's technical systems. These will be recorded.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to academy technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password, who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- ICA technical systems are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. *N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.*
- The academy has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc).
- Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.

- An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- A significant smoothwall concern would be highlighted a direct call will go straight to Catherine Jones (Designated Safeguarding Lead). If this is staff, it goes directly to the Principal.
- Appropriate security measures are in place (schools/academies may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. 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 devices are protected by up-to-date virus software.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below)
- 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/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the academy's and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Specific student/staff misuse

Where a student misuses the academy's ICT systems or internet, we will follow the procedures set out in our policies on ,behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the academies ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures/staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Any review will need to understand:

- the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what your filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of your pupils
- teaching requirements, for example, your RHSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies you have in place
- what checks are currently taking place and how resulting actions are handled

1.3.5. Key Responsibilities of Children and Young People

- Contributing to the development of online safety policies.
- Reading the academy/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

- Assessing the personal risks of using any particular technology and behaving safely and responsibly to limit those risks.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the schools/academy online safety policy covers their actions out of school, if reacted to their membership of the school.

1.3.6. Key Responsibilities of Parents/Carers

- Reading the academy/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the academy in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the academy, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the academy/setting online safety policies.
- Using academy systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
  - What are the issues? https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
  - Hot topics http://www.childnet.com/parents-and-carers/hot-topics
  - Parent factsheet https://www.childnet.com/resources/parents-and-carers-resource-sheet
  - https://www.disrespectnobody.co.uk/

2. Online Communication and Safer Use of Technology

2.1. Managing the Website

- The academy will ensure that information posted on the academy website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the academy address, email and telephone number. Staff or students' personal information will not be published.
- The Principal will take overall editorial responsibility for online content published by the academy and will ensure that content published is accurate and appropriate.
- The academy website will comply with United Learning's and the academy's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- The academy will post information about safeguarding, including online safety on the academy website, or link to the resources hosted by United Learning.
- The administrator account for the academy website will be safeguarded with an appropriately strong password.

- Email addresses will be published carefully online, to avoid being harvested for spam (eg by replacing '@' with 'AT'.)
- Pupils' work will only be published with their permission or that of their parents/carers.

2.2. Publishing Images Online

- ICA will ensure that all images are used in accordance with the academy's Image Use Policy.
- In line with the academy's Image Use Policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.
- Any images, videos or music posted online will comply with the intellectual property rights and copyright

2.3. Managing Email

- Students may only use academy/setting provided email accounts for educational purposes.
- All members of staff are provided with a specific academy/setting email address to use for any official communication.
- Staff are permitted to contact students via their own academy email account and students' academy email accounts.
- Staff must demonstrate safe and responsible online behaviour, at all times.
- If communication by a student is deemed to be personal or inappropriate, staff should not respond and the line manager or safeguarding team should be alerted immediately
- The use of personal email addresses by staff for any official academy/setting business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the academy community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the academy online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Caution should be taken on opening emails with attachments or clicking on links within; being conscious of the risks from malware.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on academy headed paper would be.
- Academy email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4. Distance Learning

- To support the safety of students, parents and staff with remote learning, an additional Acceptable User Policy has been created.

Parents

- Teams activity is analysed and reported for inappropriate content or concerning activity to ensure all students accessing Teams are following the expectations for students outlined below.
- Students who do not adhere to the above expectations may be removed from the online live lesson and will be referred to the Head of Department/Head of Year/SLT/Principal to take appropriate action and parents will be contacted.

- In addition to the Irlam and Cadishead Academy Acceptable Use Policy, students also have to adhere to a Distance Learning Acceptable use Policy. Therefore, when students are using Microsoft Teams students need to.
- Parents and are not expected to take part in the remote learning, the expectations are that you are there to support and encourage your child to take part and complete work set.

Students

- There is an expectation that students will engage in online collaborative work when requested by their teacher.
- Students will work in a respectful and helpful manner, following instructions carefully.
- The recording of still images, filmed images or audio of staff or other students without permission, and the distribution of such images, is strictly forbidden.
- Making inappropriate, offensive or unkind comments, including through emojis and/or images, will not be tolerated.
- Students must not interfere with another students work without their permission, whether it is work submitted on a platform or shared work in a collaboration space. ALL work on a platform must have managed access to restrict user access.
- When submitting academic work, students must adhere to the usual standards of academic honesty and be careful not to plagiarise work, avoiding copying off the internet and submitting as their own assignment work, or submitting work as their own without reference to co-authors if the work was generated collaboratively.

Staff

- Staff also have an additional Acceptable Use Policy for Distance Learning.
- Staff will start and end the online live lesson.
- Remote learning can be a live lesson/ voice over lesson. Staff need to consider the setting they conduct the live lesson from and use the blur tool if necessary to protect their surroundings.
- Staff will be in control of the webcam and discussion function at all times.
- The live online lesson will be monitored closely at all times.
- Leaders will be monitoring remote learning, in terms of joining lessons, quality assure the paper resources for students.

- Behaviour when working as part of an online live lesson should be as expected in normal classroom learning.
    - ☐ Respect for all participants
    - ☐ Quietly attentive
    - ☐ Prepared to ask and answer academic questions
    - ☐ Attempt learning tasks in good faith, whatever the challenge
    - ☐ Engage respectfully and enthusiastically with others when collaborating

2.5. Appropriate Safe Classroom Use of the Internet and Associated Devices

- The academy's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- Students will use age and ability appropriate tools to search the Internet for content.
- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole academy curriculum.
- The academy will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.

- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use are essential.
- All academy owned devices will be used in accordance with the academy Acceptable Use Policy and with appropriate safety and security measure in place.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The academy will use age-appropriate search tools as decided by the academy following an informed risk assessment to identify which tool best suits the needs of our community.
- The academy will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-academy/setting requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

2.6. Management of Academy Learning Platforms (LP)

- SLT, ELT and staff will regularly monitor the usage of the LP by students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current student, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP. Please also refer to the point raised regarding licensing and software settings to ensure filtering and monitoring systems are secure.
- When staff, students etc. leave the academy their account or rights to specific academy areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
    a) The user will be asked to remove any material deemed to be inappropriate or offensive.
    b) The material will be removed by the site administrator if the user does not comply.
    c) Access to the LP for the user may be suspended.
    d) The user will need to discuss the issues with a member of leadership before reinstatement.
    e) A student's parent/carer may be informed.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

2.7. Education and training

- Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students is online safety/digital literacy is therefore an essential part of the academy online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.
- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progressions, with opportunities for creative activities and will be provided in the following ways:

a) A planned online safety curriculum should be provided as part of Computing/PSHE/other lessons and should be regularly revisited.
b) Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.

The curriculum for each phase is as follows:

- The introduction of the new relationships and sex education (RSE) curriculum was compulsory from September 2020 as planned for school to deliver it. Summary of the new phrase, relationships and sex education and health education in secondary schools is compulsory.

Secondary schools

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

2.8. Protecting children from online abuse

Taken from the NSPCC “Protecting children from online abuse”(23.12.2020)

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging

- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This could happen if the original abuse happened online or offline. Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

Cyberbullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Emotional Abuse

Emotional abuse is emotional maltreatment of a child, which has a severe and persistent negative effect on the child's emotional development (Department for Education, 20171; Department of Health, 20172; Scottish Government, 20143; Wales Safeguarding Procedures Project Board, 20194). It's also known as psychological abuse.

Most forms of abuse include an emotional element, but emotional abuse can also happen on its own. Children can be emotionally abused by anyone:

- parents or carers
- family members
- other adults
- other children

Online examples of emotional abuse can include (but are not limited to):

- verbal humiliation
- name-calling
- criticism
- restricting social interaction
- exploiting or corrupting
- encouraging a child to take part in criminal activities
- forcing a child to take part in activities that are not appropriate for their stage of development
- terrorising
- threatening violence
- bullying
- deliberately frightening a child
- deliberately putting a child in a dangerous situation

Consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery);

This is when people share a sexual message and/or a naked or semi-naked image, video or text message with another person. It's also known as nude image sharing.

Children and young people may consent to sending a nude image of themselves. They can also be forced or coerced into sharing images by their peers or adults online.

If a child or young person originally shares the image consensually, they have no control over how other people might use it.

If the image is shared around peer groups, it may lead to bullying and isolation. Perpetrators of abuse may circulate a nude image more widely and use this to blackmail a child and/or groom them for further sexual abuse.

It's a criminal offence to create or share explicit images of a child (anyone under the age of 18), even if the person doing it is a child. If reported to the police, they will make a record but may decide not to take any formal action against a young person.

Sexual abuse

Child sexual abuse (CSA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline (Department for Education, 2018; Department of Health, Social Services and Public Safety, 2017; Scottish Government, 2014; Wales Safeguarding Procedures Project Board, 2019). Children and young people may not always understand that they are being sexually abused.

Contact abuse involves activities where an abuser makes physical contact with a child. It includes:

- sexual touching of any part of the body, whether the child is wearing clothes or not
- forcing or encouraging a child to take part in sexual activity
- making a child take their clothes off or touch someone else's genitals
- rape or penetration by putting an object or body part inside a child's mouth, vagina or anus

Non-contact abuse involves activities where there is no physical contact. It includes:

- flashing at a child
- encouraging or forcing a child to watch or hear sexual acts
- not taking proper measures to prevent a child being exposed to sexual activities by others
- making a child masturbate while others watch
- persuading a child to make, view or distribute child abuse images (such as performing sexual acts over the internet, sexting or showing pornography to a child)
- making, viewing or distributing child abuse images
- allowing someone else to make, view or distribute child abuse images
- meeting a child following grooming with the intent of abusing them (even if abuse did not take place)
- sexually exploiting a child for money, power or status (child sexual exploitation).

Child Sexual Exploitation

Child sexual exploitation (CSE) is a type of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (Department for Education, 2017; NIdirect, 2018; Scottish Government, 2018; Wales Safeguarding Procedures Project Board, 2019).

Children and young people in sexually exploitative situations and relationships are persuaded or forced to perform sexual activities or have sexual activities performed on them in return for gifts, drugs, money or affection.

CSE can take place in person, online, or using a combination of both.

Perpetrators of CSE use a power imbalance to exploit children and young people. This may arise from a range of factors including:

- age
- gender
- sexual identity
- cognitive ability
- physical strength
- status
- access to economic or other resources (Department of Education, 2017).

Sexual exploitation is a hidden crime. Young people have often been groomed into trusting their abuser and may not understand that they're being abused. They may depend on their abuser and be too scared to tell anyone what's happening because they don't want to get them in trouble or risk losing them. They may be tricked into believing they're in a loving, consensual relationship.

When sexual exploitation happens online, young people may be persuaded or forced to:

- have sexual conversations by text or online
- send or post sexually explicit images of themselves
- take part in sexual activities via a webcam or smartphone (Hamilton-Giachritsis et al, 2017).

Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in further sexual activity. Images or videos may continue to be shared long after the sexual abuse has stopped.

Radicalisation

Information taken from: https://www.getsafeonline.org/social-networking/online-radicalisation/

Radicalisation by extremist groups or individuals can be perpetrated via several means: face-to-face by peers, in organised groups in the community and, increasingly, online. Their targets are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

However, extremists attempt to influence vulnerable people, the internet invariably plays some kind of role it can be used both to create initial interest, and as reinforcement to other means of communication. As is the case with everything it is used for, the internet enables considerably larger numbers of people to be reached, in a wider geographic area, and with less effort by the perpetrators.

The power of social media is well-known, and it is this that is the main channel for such grooming – be it Facebook, Twitter or the multitude of other sites and apps. Other online channels include chatrooms, forums, instant messages and texts. All are also used by extremists for their day-to-day communication, as is the dark web.

Social media is also used for research by extremists, making it easy for them to identify those who may be vulnerable from what they reveal in their profiles, posts/tweets, photos and friend lists.

The Academy's response to online abuse

- To help prevent online abuse we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The academy will actively discuss examples of online abuse with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover examples of online abuse. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on examples of online abuse its impact and ways to support pupils, as part of safeguarding training.
- The school also sends information/leaflets on examples of online abuse to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of online abuse, the academy will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

3. Policy Decisions

3.1. Recognising Online Risks

- Irlam and Cadishead Academy is aware that the Internet is a constantly changing environment with new apps,
  tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the academy leadership team will ensure that appropriate risk assessments are carried out before use in academy is allowed.
- The academy will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content. Academy's should include appropriate details about the systems in place.
- The academy will audit technology use to establish if the Online Safety (e–Safety) Policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the academy's leadership team.
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the academy's leadership team.

3.2. Internet Use Within the Community

- The academy will liaise with United Learning and local feeder academy's to establish a common approach to online safety (e–Safety).
- The academy will provide an Acceptable Use Policy for any guest/visitor who needs to access the academy computer system or internet on site.

3.3. Authorising Internet Access

- The academy will maintain a current record of all staff and students who are granted access to the academy's electronic communications.
- All staff, students and visitors will read and sign the Academy Acceptable Use Policy before using any academy ICT resources.
- Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Academy Acceptable Use Policy for student access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the academy community (such as with children with special education needs) the academy will make decisions based on the specific needs and understanding of the student(s).

4. Engagement Approaches

4.1. Engagement of Children and Young People

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole academy, to raise awareness regarding the importance of safe and responsible internet use amongst students.
- Education about safe and responsible use will precede internet access.
- Students input will be sought when writing and developing academy online safety policies and practices.
- Students will be supported in reading and understanding the academy Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Student instruction regarding responsible and safe use will precede Internet access.
- Online safety (e-Safety) will be included in the Citizenship and Computing programmes of study covering both safe academy and home use.
- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- The student Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the academy's internal online safety (e-Safety) education approaches.
- The academy will reward positive use of technology by students.
- The academy will implement peer education to develop online safety as appropriate to the needs of the students.

4.2. Engagement of Staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of academy safeguarding practice.
- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.

- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy online safety policy and acceptable user agreements.
- To protect all staff and students, the academy will implement Acceptable Use Policies which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the leadership team and will have clear procedures for reporting issues or concerns.
- The academy will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.
- Training- Staff are provided with training and opportunities to practice using software/systems intended to be implemented during remote learning. Training is on going led through the Teaching and Learning team on effective pedagogies they can use in an online environment.
- All members of staff will be made aware that their online conduct out of academy could have an impact on their role and reputation within academy. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

4.3 Engagement of Parents/Carers

- This policy will be shared with parents/carers.
- Irlam and Cadishead Academy recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the academy's Online Safety (e-Safety) policy and expectations in newsletters, the academy prospectus, social media and on the academy website.
- Parents will be requested to read online safety information as part of the Home Academy Agreement.
- Parents will be encouraged to read the academy Acceptable Use Policy for students and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.
- Training- Parents/carers will also receive training in school methodology in using Office 365, Teams, Streams etc.
- Parents will be receive regular communication through various systems, twitter, facebook group, website, email/letter with regarding Microsoft Office 365 tools and expectations from students .High profile events/campaigns e.g.: Safer Internet Day. Reference to the relevant web sites/publications. Curriculum meetings.

5. Responding to Online Incidents and Concerns

- All members of the academy/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to the United Learning Designated Safeguarding Officer and relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the Academy's complaints procedure.
- Complaints about online bullying will be dealt with under the Academy's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the Principal
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Students, parents and staff will be informed of the academy's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the academy community will need to be aware of the importance of confidentiality and the need to follow the official academy procedures for reporting concerns.
- All members of the academy community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the academy community.
- The academy will manage online safety (e-Safety) incidents in accordance with the academy discipline/behaviour policy where appropriate.
- The academy will inform parents/carers of any incidents of concern as and when required.
- After any investigations are completed, the academy will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the academy will contact the Local Education Safeguarding Team or Local Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to United Learning Technology Team and Local Police.
- If the academy is unsure how to proceed with any incidents of concern, then the incident will be escalated to the United Learning Lead Safeguarding Officer or Local Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the academy, then the concern will be escalated to the Local Education Safeguarding Team to communicate to other academy's/settings in area.
- Parents and children will need to work in partnership with the academy to resolve issues.

Contacts and References:

- Keeping Children Safe in Education https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Teaching online safety in schools https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- Child Exploitation & Online Protection Centre www.ceop.gov.uk/
- Think U Know website www.thinkuknow.co.uk
- NSPCC www.nspcc.org.uk/html/home/needadvice/needadvice.htm
- Preventing and tackling bullying https://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Searching, screening and confiscation https://www.gov.uk/government/publications/searching-screening-and-confiscation
- Protecting children from radicalisation https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty
- Meeting digital and technology standards in schools and colleges https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
- Cyber-bullying: advice for headteachers and school staff https://www.gov.uk/government/publications/preventing-and-tackling-bullying Relationships and sex education https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education
- United Learning Hub website
- Department of Education: Teaching online in academy-review revised document September 2020.
- National Cyber Security Centre (Weekly threat report)
- UL Copyright Policy Link to United Learning Copyright Policy: https://hub.unitedlearning.org.uk/sites/policies/Technology%20Policies/Copyright%20and%20PRS.docx
- UL Using your own device policy (BYOD/BYOT) *https://hub.unitedlearning.org.uk/sites/policies/Technology%20Policies/Accessing%20United%20Learning%20Data%20Using%20your%20Own%20Device%20Policy.docx*