Adult Learning Kirklees

Online Safety Policy

2022-2024

Adult Learning Kirklees is part of Kirklees Council and as such follows all KC policies, procedures and guidance.

All policies will be reviewed annually by the ALK Advisory Board unless there are in year changes required according to legislation or policy change.

Providers will be made aware of any new policies or changes to inform and amend their own policies and guidance. Policies highlighted will need to be devised, reviewed and revised by the provider annually.

Policies created by: Jeanette Palmer Nina Barnes	Date Created: July 2022	Date of Renewal: July 2024

Table of Contents

Safeguarding Children

www.kirkleessafeguardingchildren.co.uk/procedures-local-protocols-and-guidance

1. Introduction

This online safety policy recognises the commitment to keeping staff and learners safe online and acknowledges its part in ALK's overall safeguarding policies and procedures. We believe the learning community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The online safety policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group.

(DfE Keeping Children Safe in Education 2021)

This policy shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the learning community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken.

Our expectations for responsible and appropriate conduct are set out in our Acceptable Use Policies (AUP) which we expect all staff and learners to follow.

As part of our commitment to online safety we also recognise our obligation to implement a range of security measures to protect the network and facilities from attack, compromise and inappropriate use and to protect data and other information assets from loss or inappropriate use.

The scope of this policy

- This policy applies to the ALK community including the ALK Team (SLT), Advisory Board(AB), all staff employed directly or indirectly, volunteers, visitors and all learners.
- The ALK team and AB will ensure that any relevant or new legislation that may impact upon the provision for online safety within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers leaders to such extent as is reasonable, to regulate the behaviour of learners when they are off the site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety related incidents covered by this policy, which may take place out of sessions. ALK will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies.

ALK DSO is Jeanette Palmer/ Deputies are Nina Barnes and Nadine Littlewood.

Implementation of the policy

- The ALK Team will ensure all members of staff are aware of the contents of the Online Safety Policy and the use of any new technology.
- All staff, learners, occasional and external users of ICT equipment will sign the relevant Acceptable Use Policies at provider centres.
- All amendments will be raised at awareness sessions at provider meetings.
- Online safety will be part of the curriculum for learners.
- Online safety posters will be prominently displayed in venues.
- The Online Safety Policy will be made available via the website.

The following local and national guidance are acknowledged and included as part of our Online Safety Policy:

1. **Kirklees LSCP Guidance**

The Kirklees Safeguarding Children's Partnership Procedures and Guidance

Kirklees Safeguarding procedures will be followed where an online safety issue occurs which gives rise to any concerns related to child protection. In particular we acknowledge the specific guidance in:

Section 1.4.5 Child Abuse and Information Communication Technology

This section of the Kirklees Safeguarding procedures covers awareness of, and response to, issues related to child abuse and the internet. In particular we note and will follow the advice given in the following section:

Section 7 Actions to be taken where an Employee has Concerns about a Colleague
This provides guidance on the action to be taken if an employee has either information or reason to suspect that a colleague is accessing indecent images of children.

2. Government Guidance

Keeping Children Safe in Education (DfE 2021) with particular reference to Annex D Online Safety

Teaching Online Safety in School (DfE 2019)

The Prevent Duty: for schools and childcare providers (DfE 2015)

Revised Prevent Duty Guidance for England and Wales (Home Office 2015)

How social media is used to encourage travel to Syria and Iraq - Briefing note for schools (DfE 2015)

Cyberbullying: Advice for Headteachers and School Staff (DfE 2014)

Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfE 2020)

Sexual violence and sexual harassment between children in schools and colleges (DfE 2021)

3. Kirklees Learning Service Guidance

The following Kirklees guidance documents are included as part of this Online Safety Policy:

Kirklees Electronic Communications Guidance for Staff

4. Other Guidance

Appropriate Filtering for Education Settings (UK Safer Internet Centre)

2. Responsibilities of the ALK community

We believe that online safety is the responsibility of the ALK community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The leadership team accepts the following responsibilities:

- The ALK DSO and advisory board will take ultimate responsibility for the online safety of the ALK community through raising awareness and ensuring systems and policies are in place.
- Ensure policies and procedures are in place to ensure the integrity of ALK information and data assets.
- Ensure liaison with the board members.
- Develop and promote an online safety culture within the ALK community.
- Ensure that all staff, learners and other users agree to the Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the ALK community to ensure they are able to carry out their roles effectively with regard to online safety
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur and review incidents to see if further action is required

Responsibilities of the Designated Safeguarding Leads (DSO)

- Be the first point of contact for online safety issues at each provider venue.
- Be aware of and understand the risks from online activities such as grooming for sexual exploitation, sexting, online bullying, radicalisation and others.
- Attend regular training and updates on online safety issues. Stay up to date through use of online communities, social media and relevant websites/newsletters.
- Ensure delivery of an appropriate level of training in online safety issues each year and throughout the year at cpd events and provider meetings.
- Create and maintain online safety policies and procedures.

- Ensure that staff and learners know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident.
- Liaise with the Local Authority, the Local Safeguarding Children's/ Adults Partnership and other relevant agencies as appropriate.
- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.
- Raise awareness of the particular issues which may arise for vulnerable learners in the approach to online safety.

Responsibilities of all Staff

- Read, understand and help promote the online safety policies and guidance
- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive data and information
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with learners is on a professional level and only through work based systems, **NEVER** through personal email, text, mobile phone, social network or other online medium
- Embed online safety messages in learning activities where appropriate
- Supervise learners when engaged in learning activities involving technology
- Ensure that learners know what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all online safety incidents which occur in the appropriate log and/or to their line manager and ALK DSO
- Respect, and share with learners the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Responsibilities of Learners

- Read, understand and adhere to the AUP and follow all safe practice guidance
- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of sessions
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in sessions and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
    - To use their own e-mails and devices and understand that cameras should be turned on in the classroom environment, unless there is a specific reason as discussed and agreed with the tutor beforehand
- To know, understand and follow policies/ guidance on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow policies/ guidance regarding online bullying

Responsibilities of the Governing Body

- Read, understand, contribute to and promote the online safety policies and guidance as part of ALK's overarching safeguarding procedures
- Support the work in promoting and ensuring safe and responsible use of technology in and out of sessions, including encouraging learners to become engaged in online safety awareness
- To have an overview of how the IT infrastructure provides safe access to the internet and the steps ALK takes to protect personal and sensitive data

Responsibility of any external users of the systems

- Take responsibility for liaising with ALK on appropriate use of the IT equipment and internet, including providing an appropriate level of supervision where required
- Ensure that participants follow agreed Acceptable Use Procedures

Acceptable Use Policies

ALK has a number of AUPs for different groups of users.

These are shared with all users yearly and staff and learners will be expected to agree to them and follow their guidelines. External groups and visitors who use our ICT facilities are made aware of the appropriate AUP.

See separate AUPs.

3. Training

Technology use changes at a fast pace, and we recognise the importance of regular staff training. The DSOs will attend regular training updates as necessary, and keep up to date through online resources, newsletters and networks. All staff will receive regular updates on risks to learners online from the DSO, and attend online or external training as necessary. Regular DSO meetings will ensure awareness of online safety and any relevant updates and issues.

4. Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our learning community lies in effective education. We know that the internet and other technologies are embedded in our lives, not just in sessions but outside as well, and we believe we have a duty to help prepare them to benefit safely from the opportunities that these present.

We deliver online safety knowledge and understanding and to ensure that learners have a growing understanding of how to manage the risks involved in online activity. Online safety is embedded across the curriculum, with learners having relevant opportunities to apply their skills.

We discuss, remind or raise relevant online safety messages with learners routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind learners about the responsibilities to which they have agreed through the AUP.

learners will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

5. Remote education and home learning

Online learning will continue to be used as part of a blended offer. All Acceptable Use Policies will apply to resources which are accessed in the home environment.

The following DfE guidance will be used:

Safeguarding and remote education during coronavirus (COVID-19), DfE March 2021 as appropriate.

6. Managing and Safeguarding IT systems

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for learning activity.

All administrator or master passwords for IT systems are kept secure and available to at least two members of staff as appropriate.

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named staff. We do not allow anyone except technical staff to download and install software onto the network.

Filtering

In order to be compliant with the Prevent Duty and Safeguarding Children in Education 2016, the provider will:

- As part of the Prevent duty, carry out an annual assessment of the risk to pupils of exposure to extremist content as part of the Prevent RA.

Ensure that all reasonable precautions are taken to prevent access to illegal and extremist content. Web filtering of internet content is provided by council systems/ provider systems. However it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in learners in monitoring their own internet activity.

- Inform all users about the action they should take if inappropriate material is accessed or discovered on a computer. Deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

- Expect teachers to check websites they wish to use prior to lessons to assess the suitability of content.
- Post notices in classrooms as a reminder of how to seek help.

Monitoring

In order to be compliant with the Prevent Duty and Keeping Children Safe in Education 2021, the school will:

- Use the findings of the annual Prevent risk assessment to put appropriate internet and network monitoring systems in place.
- Learners are supervised by staff while using the internet in sessions where possible as this reduces the risk of exposure to extremist, illegal or inappropriate material; direct supervision also enables staff to take swift action should such material be accessed either accidentally or deliberately.
- Learners are made aware of risks to ensure they are prepared and informed and know who to report any concerns to.

Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, management information system).
- All staff and learners have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- The provider maintains a log of all accesses by users and of their activities while using the system in order to track any online safety incidents.

7. Using the internet

We provide the internet to

- Support teaching, learning and curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the IT systems and that such activity can be monitored and checked.

All users of the IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Learners and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms.

Using email

Email is regarded as an essential means of communication. Email messages on ALK business should reflect a suitable tone and content and should ensure that the good name of ALK is maintained.

It is the personal responsibility of the email account holder to keep their password secure.

As part of the IT curriculum learners are taught about safe and appropriate use of email.

Responsible use of personal web mail accounts on learning systems is permitted outside teaching hours.

Publishing content online

E.g. using websites, learning platforms, blogs, wikis, podcasts, social network sites, livestreaming

Permission from learners to use their work, photographs and identity should be gained.

Creating online content as part of the curriculum:

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the sessions:

Staff and learners are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing.

Material published by learners, governors and staff in a social context which is considered to bring ALK into disrepute or considered harmful to, or harassment of another learner or member of the community will be considered a breach of discipline and treated accordingly.

Using video conferencing, web cameras and online meeting apps

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up. We ensure that staff and learners take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

For their own protection a video conference or other online meeting between a member of staff and learners which takes place outside sessions or whilst the member of staff is alone is always conducted with the prior knowledge of the line manager.

Using mobile phones

Personal devices are brought onto premises by learners at their own risk.

During lesson time we expect all mobile phones belonging to staff to be switched off unless there is a specific agreement for this not to be the case. Learners should also follow guidance as to using mobiles in sessions.

Unauthorized or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another learner or staff member we do not consider it a defense that the activity took place outside session hours.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress is online bullying; this will be considered a disciplinary matter.

Using wearable technology

Wearable technology includes electronic fitness trackers and internet enabled ‘smart’ watches. Wearable technology can be used as agreed with tutors. The provider does not accept liability for loss or damage of personal devices.

Wearable technology is not to be worn during tests or examinations.

Using mobile devices

We recognise that the multimedia and communication facilities provided by mobile devices (e.g. iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities. However their use in lesson time will be with permission from the teacher and within clearly defined boundaries.

Using other technologies

We will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an online safety point of view.

We will regularly review the online safety policy to reflect any new technology that we use, or to reflect the use of new technology. Staff or learners using a technology not specifically mentioned in this policy, or a personal device whether connected to the network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

8. Protecting data and information

ALK recognises the obligation to safeguard staff and learner sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

Learners are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the management information system holding data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside work
- All devices taken off site, e.g. laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- We follow Kirklees' procedures for transmitting data securely and sensitive data is not sent via emailed unless encrypted
- Remote access to computers is by authorized personnel only
- We have full back up and recovery procedures in place for data

- Where sensitive staff or learner data is shared with other people who have a right to see the information, for example governors or Kirklees officers, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

Management of assets

Details of all hardware and software are recorded in an inventory.

All redundant IT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2013.

Responding to online safety incidents

All online safety incidents are recorded in the monthly Safeguarding Log which is regularly reviewed.

In situations where a member of staff is made aware of a serious online safety incident concerning learners or staff, they will inform the DSO.

Instances of **online bullying** will be taken very seriously by the and dealt with using anti-bullying procedures. ALK recognises that staff as well as learners may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about child protection or the discovery of indecent images on the computer, then the procedures outlined in the Kirklees Safeguarding Procedures and Guidance will be followed.

Section 1.4.4 Child Abuse and Information Communication Technology

Dealing with complaints and breaches of conduct:

Any complaints or breaches of conduct will be dealt with promptly

- Responsibility for handling serious incidents will be given to the DSL and a senior member of staff
- Learners will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, in breach of the Equalities Act or violent/threatening violence
- online peer on peer abuse and sexual harassment
- continuing to send or post material regarded as harassment or of a bullying nature after being warned
- staff using digital communications to communicate with learners in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to log in using your account
- accessing ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

9. Reviewing online safety

An annual review of online safety policy and practice can be carried out using the 360 Safe self-review tool: https://360safe.org.uk/

ALK review the online safety policy and update and amend informed by the Online Safety for Kirklees Schools.