

Venture Learning

IT & Online Safety Policy

Venture Learning

Document Owner	Rhys Griffiths
Version	1.0
Effective From	21/01/2019
Next Review Date	21/01/2020

Introduction

This policy is set out in accordance with the online safety principles laid out in *Keeping Children Safe in Education* statutory guidance document (DfE, 2018):

> 'The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.
>
> An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.
>
> The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
>
> • 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.'

At Venture Learning, we recognise that the complex nature of our students increases the possibility that they may have already, or are likely to be exposed to any/all of these risks online. We take a proactive approach to online safety: embedding it throughout our curriculum; positively modelling the safe and appropriate use of ICT; and, addressing areas of concern with targeted, direct work.

This policy lays out the measures that Venture Learning will take to minimise the risks posed to students online as well as to recognise and respond effectively to any online activity that puts young people at risk.

Key Staff and Contacts

Name	Role
Rhys Griffiths	**Head of Provision**
Holly Crann	**Deputy Head of Provision**
Rhys Griffiths	Designated Safeguarding Lead
Holly Crann	Deputy Designated Safeguarding Lead
Holly Crann	Online Safety Lead
Contact details:	**Venture Learning** **19A Forester Street** **Netherfield** **Nottingham** **NG4 2LJ**
	www.venturelearning.co.uk
	0115 987 6621 / 07587 408 996
	Rhys.griffiths@venturelearning.co.uk
	Holly.crann@venturelearning.co.uk

Section 1: Roles and Responsibilities

Venture Learning is ultimately responsible for ensuring that the outside contractor managing the ICT service has carried out all necessary online safety measures, including but not limited to:

• ensuring the technical infrastructure is secure and is not open to misuse or malicious attack;

• meeting the required online safety technical requirements of the Local Authority;

• ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;

• applying and updating the filtering policy

• implementing monitoring software/systems as agreed with Venture Learning;

• reporting any misuse/ attempted misuse of the ICT system to the Provision Lead.

1.1. Online Safety Lead

Takes responsibility for:

• taking day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents;

• ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;

• providing training and advice for staff; and,

• receiving reports of online safety incidents and creates a log of incidents to inform future online safety developments.

1.2. Teaching and Support Staff

Are responsible for ensuring that:

• they have an up to date awareness of online safety matters and of the current Venture Learning Online Safety Policy and practices

• they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)

• they report any suspected misuse or problem to the Provision Lead for investigation

• all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official systems

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

• students understand and follow the Online Safety Policy and acceptable use policies

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

• in lessons where internet use is pre-planned students should be 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

1.3. Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data
• access to illegal / inappropriate materials
• inappropriate on-line contact with adults / strangers
• potential or actual incidents of grooming
• online-bullying

1.4. Students

All students must:

• use the Venture Learning digital technology systems in accordance with the Student Acceptable Use Agreement;

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

• know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying;

• understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Venture Learning's Online Safety Policy covers their actions when off-site, if at all related to their attendance at the provision.

1.5. Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use internet/mobile devices in an appropriate way. Venture Learning will take every opportunity to help parents understand these issues through communication with home. Parents and carers will be encouraged to support the Venture Learning in promoting good online safety practice.

Section 2: Operation of the Policy

2.1. Online Safety in the Curriculum

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 in online safety and digital literacy is therefore an essential part of Venture Learning's online safety provision. Young people need the help and support of their educational provision 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 progression, with opportunities for creative activities and will be provided in the following ways:

• a planned online safety curriculum should be provided as part of ICT, PSHE and other lessons and should be regularly revisited;

• key online safety messages should be regularly reinforced as part of pastoral activities;

• students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information;

• students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the provision;

• staff should act as good role models in their use of digital technologies, the internet and mobile devices;

• in lessons where internet use is pre-planned, it is best practice that students / pupils should be 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

2.2. Online Safety Training for Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Venture Learning's Online Safety Policy and Acceptable Use Agreements;

• the Online Safety Lead (or other nominated person) will receive regular updates by reviewing guidance documents released by relevant organisations;

• this Online Safety Policy and its updates will be presented to and discussed by staff as part of ongoing CPD;

• the Online Safety Office Lead will provide advice/guidance/training to individuals as required.

2.3. Technical: Infrastructure, Equipment, Filtering and Monitoring

Venture Learning will be responsible for ensuring that the on-site infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

• technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements;

• regular reviews and audits of the safety and security of technical systems;

• servers, wireless systems and cabling must be securely located and physical access restricted;

• all users will have clearly defined access rights to technical systems and devices;

• all users will be provided with a username and secure password by and an up-to-date record of users and their usernames will be maintained. Users are responsible for the security of their username and password and will be required to change their password every 90 days;

• the "master / administrator" passwords for the ICT systems, used by the Network Manager (or other person) must also be available to the Provision Lead and kept in a secure place;

• Provision Lead is 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;

• 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. There is a clear process in place to deal with requests for filtering changes;

• internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet;

• 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 for users to report any actual or potential online safety breaches;

• an agreed system is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

2.4. Mobile Technologies (including BYOD)

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, notebook/laptop or any other technology that has the capability of accessing Venture Learning's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage. See Appendix 1 for information about device access.

All users must understand that the primary purpose of the use mobile and personal devices in on-site is educational. Venture Learning's Acceptable Use Agreements for staff, students and parents/carers will give consideration to the use of mobile technologies.

Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Online Safety curriculum.

2.5. Use of digital and video images

Staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• when using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;

• written permission from parents or carers will be obtained before photographs of students are published on Venture Learning's website and social media;

• staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Venture Learning's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on the centre's equipment, the personal equipment of staff should not be used for such purposes;

• students must not take, use, share, publish or distribute images of others without their permission;

• photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images;

• students' full names will not be used anywhere on a website or social media, particularly in association with photographs.

2.6. Digital Communication

When using communication technologies Venture Learning considers the following as good practice:

• the official Venture Learning email service may be regarded as safe and secure and is monitored. Users should be aware that email communications may be monitored. Staff and students should therefore use only the email service to communicate with others about professional matters;

• users must immediately report, to the nominated person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;

• any digital communication between staff and students or parents/carers must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications;

• students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Personal information should not be posted on the Venture Learning website and only official email addresses should be used to identify members of staff.

2.7. Social Media: Maintaining Professional Identity
Venture Learning provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the provision through:

• ensuring that personal information is not published;

• training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues;

• clear reporting guidance, including responsibilities, procedures and sanctions;

• risk assessment, including legal risk

Venture Learning staff should ensure that:

• no reference should be made in social media to students, parents/carers or staff;

• they do not engage in online discussion on personal matters relating to members of the Venture Learning community;

• personal opinions should not be attributed to Venture Learning;

• security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy; Venture Learning permits reasonable and appropriate access to private social media sites.

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the Venture Learning. Nominated persons at Venture Learning should appropriately and effectively respond to social media comments made by others. Venture Learning's use of social media for professional purposes will be reviewed regularly to ensure compliance with its policies and vision.

2.8. Dealing with unsuitable / inappropriate activities
The misuse of IT by a student or a member of staff can constitute a safeguarding risk. Staff or students should pass any concerns in this area to the DSL. Venture Learning will apply normal safeguarding procedures for investigating any concerns in this area. Please refer to Appendix 2 of the 'Arrangements for Safeguarding and Child Protection at Venture Learning' policy.

Appendix 1

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes/No*	*Yes/No*	*Yes/No*
Full network access	*Yes*	*Yes*	*Yes*			
Internet only						
No network access						