# Online Safety Policy

## Version 1: May 2020

[Insert school name]

Delete and replace with school logo

| | |
|---|---|
| **Date approved by Trustees of Ventrus Multi Academy Trust** | **20 May 2020** |
| **Review Period** | **2-yearly** |
| **Next Review Date** | **May 2022** |
| **Signed by Chair of Trustees Hugh Whittaker** |  |

**CONTENTS**

# 1. AIMS

Ventrus aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and across our governance structures
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

# 2. APPROACH

New technologies have become integral to the lives of children and young people in today's society, both within their academic lives and also in their lives away from academia. We want young people to be able to fully utilise the benefits offered by ICT while doing so in a safe manner.

Online messaging, social networking and mobile technology effectively mean that children can always be 'online'. Their social lives, and therefore their emotional development, are bound up in the use of these technologies. Latest e-safety guidance states that the breadth of e-safety issues can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

The purpose of this policy is to ensure that Ventrus schools are kept aware of the risks, as well as the benefits, of technology and how to manage these risks and keep themselves and others safe. It details the measures that the schools have put in place to support this, as well as the rules and restrictions around the use of ICT and other technology across Ventrus.

# 3. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

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

The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

# 4. ROLES AND RESPONSIBILITIES

## 4.1 Board of Trustees and Local Governing Bodies

The Board of Trustees will have overall responsibility for monitoring this policy and ensuring the systems are in place for holding the Headteachers to account for its implementation.

The Headteachers/Senior NST staff will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs, as provided by the designated safeguarding lead (DSL). The Local Safeguarding Governor will oversee online safety. At [name of school] this person is [add name].

All Trustees and Local Governors will:

- Ensure that they know the policy is in place and understand how the policy is managed at the individual school level.
- Agree and adhere to the terms defined in the Acceptable Use Agreement of Ventrus ICT systems and the internet.

## 4.2 The Headteacher (is also the Designated Safeguarding Lead in Ventrus schools)

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented.

As DSL, the Headteacher takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Linking with the Local Safeguarding Governor
- Working with TME/ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the schools' behaviour policies
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or Local Governing Body

This list is not intended to be exhaustive.

## 4.3 The IT Team

Pilton network manager/TME are commissioned to be responsible for ensuring:

- Appropriate filtering and monitoring systems, which are updated on a regular basis, keep pupils safe from potentially harmful and inappropriate content and contact online while at the school, including terrorist and extremist material.
- That all security aspects relating to IT that Ventrus' schools, including
- Antivirus/Windows updates/Backups are monitored and/or updated within a reasonable timescale of their general release availability.
- Access to potentially dangerous sites is blocked and, where possible, the downloading of potentially dangerous files is prevented.

## 4.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms of the Acceptable Use Agreement on the school's ICT systems and the internet, and ensuring that pupils follow the school's terms of the Acceptable Use Agreement.
- Working with the Headteacher to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy

This list is not intended to be exhaustive.

## 4.5 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Understand that their child, in using Ventrus ICT systems, will have read, understood and agreed to the terms of the Acceptable Use Agreement on the school's ICT systems and internet.

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

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

## 4.6 Visitors and members of the community

Visitors and members of the community who use the Ventrus IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms of the Acceptable Use Agreement.

# 5. MOBILE TECHNOLOGIES

## 5.1 Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present.

With Headteacher consent, staff personal mobile devices may be connected to the internet via the schools WiFi network. Where consent is given, Headteachers will meet with staff individually and make them aware that they are required to adhere to the Ventrus policies and procedures, when using their device.

The school is not responsible for the loss, damage or theft of any personal mobile device.

## 5.2 Managing email

- The use of email within school is an essential means of communication for staff.
- Pupils currently do not access individual email accounts within school.
- Staff must use the school's approved email system for any school business.
- Staff must inform Headteacher if they receive an offensive or inappropriate e-mail.

## 5.3 Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

## 5.4 Safe Use of Images

### 5.4.1 Creation of videos and photographs

The school permits the appropriate taking of images by staff and pupils with school equipment, in line with the ICO Guidelines, as part of their teaching.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

### 5.4.2 Publishing pupils' images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/ carers may withdraw or amend permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa on the school website, twitter account, mobile app or any other school based publicity materials.

### 5.4.3 Storage of Images

Images/ films of children will be stored securely by the school on their secure server or cloud storage, or on teacher's individual school laptops/school computers.

## 6. EDUCATING PUPILS ABOUT ONLINE SAFETY [SUBJECT CHAMPION TO ENSURE THIS IS COVERED IN COMPUTING CURRICULUM]

Pupils will be taught about online safety as part of the curriculum.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact
- on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

[Primary schools remove KS3/KS4]

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.

The safe use of social media and the internet will also be covered in other subjects where relevant, this includes safeguarding across the curriculum including supporting and minimising risk of online radicalisation and extremism.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

### 6.1 Distance Learning

Schools will ensure that a robust system is in place to facilitate distance learning through the use of trust approved secure online platforms. This platform should only be accessible by approved members of staff and students. Parents and students will be provided details of how to access the distance learning platform when the need arises. All activity through the online learning platform must conform to the trust acceptable use policy and be professional in content and tone. No personal information of students or teachers should be published to any area of the learning platform, this includes videos/photographs where an individual is identifiable, phone numbers and email addresses. Inappropriate use of the online learning platform should be reported to the Headteacher.

## 7. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

In Ventrus schools, the Headteacher , as DSL, will raise parents'/carers' awareness of internet safety in letters or other communications home, in information via school websites. This policy will also be shared with parents/carers.

Online safety will also be covered during parents'/carers' evenings/workshops.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

## 8. CYBER-BULLYING [SCHOOLS NEED TO ENSURE THIS IS REFLECTED IN THEIR BEHAVIOUR POLICIES]

### 8.1 Definition

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.)

### 8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

- Class teachers/form tutors will discuss cyber-bullying with their classes/tutor groups, and the issue will be addressed in assemblies.
- All teaching staff will find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, Local Governors and volunteers (where appropriate) will receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training
- Annually, the school will send information/leaflets on cyber-bullying 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 cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Headteacher will use all reasonable endeavours to ensure the incident is contained.
- In consultation with the Ventrus Executive Leadership Team, the Headteacher 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.

### 8.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If a member of staff suspects either of the above, they must immediately inform the Headteacher, who is responsible for deciding the appropriate course of action. Where the Headteacher takes the decision to examine a pupil's electronic device, the Headteacher must be accompanied by a member of their senior leadership team.

If inappropriate material is found on the device, it is up to the Headteacher, in conjunction with the accompanying member of the senior leadership team to decide whether they should:

- Retain it as evidence (of a criminal offence or a breach of the school Behaviour Policy), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for images or files on pupils' electronic devices will be dealt with through the Ventrus Complaints Policy and Procedure.

## 9. ACCEPTABLE USE OF THE INTERNET IN THE SCHOOL

All pupils, parents, staff, volunteers and governors are made aware of the Acceptable Use agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements.

## 10. PUPILS USING MOBILE DEVICES IN THE SCHOOL

[Adapt/remove this section to reflect your Academy approach]

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons

- Tutor group time
- Clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school by pupils must be in line with the terms of the Acceptable Use Agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Behaviour Policy, which may result in the confiscation of their device.

## 11. STAFF USING WORK DEVICES OUTSIDE OF THE SCHOOL

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the terms of the Acceptable Use Agreement, as set out in the Ventrus Code of Conduct and Ventrus Data Protection Policy

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school **MUST** be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the TME/Network Manager.

## 12. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the school Behaviour Policy. 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 school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Ventrus Conduct Policy and/or disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

In consultation with the Ventrus Executive Leadership Team, the Headteacher will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 13. TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation and extremism.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

As DSL, the Headteacher will undertake child protection and safeguarding training; they will deliver safeguarding training, at a frequency determined by the Ventrus Safeguarding Policy, to all staff. This safeguarding training will include elements of online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Local Governors will receive training on safe internet use and online safeguarding issues, as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in the Ventrus Safeguarding Policy.

## 14. FILTERS

All Ventrus internet connections are subject to internet access controls. These controls restrict the type of internet connections that can be established.

By default general web traffic (HTTP and HTTPS) is permitted. Other types of connections will be subject to review.

All web traffic is filtered as defined by filter categories in addition to whitelists and blacklists to supplement the categories where required. The filter categories must be regularly updated and include blacklists as defined by the Internet Watch Foundation.

Whilst every effort will be made to ensure inappropriate content is not accessible, Ventrus recognise that some inappropriate access could still be possible. Ventrus mitigates against the impact of this gap through appropriate education of all users, and additional safety mechanisms, such as computer monitoring software.

## 15. MONITORING ARRANGEMENTS

All connections to the internet are monitored. Where possible capturing the username, date, time and URL that is accessed. All schools use Netsweeper via Schools Broadband to monitor internet usage. The Headteacher will be informed of any concerns.

To monitor and provide enhanced filtering of the internet Ventrus will intercept and decrypt HTTPS traffic. Traffic relating to financial services and health and medicine categories will not be intercepted. Where possible computer workstations will have additional monitoring software installed.

[Secondary schools only]
This software will also:

- monitor sites accessed on the internet;
- monitor applications used on the computer;
- capture keystrokes, alerting appropriate staff to specific keywords that are typed;
- provide remote monitoring and control of computers for use by teachers and ICT services.

Ventrus computers are protected by a number of different mechanisms to keep the computers and all users safe. These protections will include:

- specific policies to limit the administrative access of the device;
- firewalls and anti-virus software to protect against malicious attack of the device;
- regular software update processes to automatically patch vulnerabilities.

## 16. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Ventrus Complaints Policy and Procedures

## Appendix 1 Policy History

| Policy Date | Summary of change | Contact | Version/ Implementation Date | Review Date |
|---|---|---|---|---|
| April 2020 | Policy rewritten to include both primary and secondary | AL | Version 1 | April 2022 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |