Salterlee Primary School

Acceptable Use of Digital Technologies Online (e-Safety) Policy 2017

Key persons:

Headteacher: Mark Scott

E-Safety Leader: Mark Scott

Governor for E-safety: Kirstien Ginesi

1. What is a Digital Technologies Online (e-Safety) AUP (Acceptable Use Policy)?

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all online technologies* for adults and children at the Academy. It explains what will happen in the event of any unacceptable use of these technologies. It also states how the school will provide support and guidance to pupils, parents/carers and families for the safe and responsible use of these technologies beyond the school setting.

*This covers any usage of the internet including mobile phone technologies.

2. Why have an AUP?

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise these risks and especially so when children use these technologies.

These risks include:

- Commercial issues with spam and other inappropriate email.
- Viruses which may compromise both Academy and personal security.
- Potentially illegal activities such as downloading copyright materials and file-sharing.
- Online content which is abusive or pornographic.
- Cyber-bullying.
- Grooming by predatory adults, usually pretending to be younger than their true age.

It is also important that staff are clear about appropriate procedures, for example, only contacting children about homework via a school email address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

The Academy acknowledges that whilst we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure that children are best protected.

As per the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the active involvement of both children and their

parents/carers is vital to the successful use of online technologies. This policy aims to inform how pupils and parents/carers are part of the procedures and how children should be educated to make good judgements about what they see, find and use. The term 'e-Safety' is used to encompass the safe use of all online technologies in order to protect children and adults from known and potential risks.

3. AUP Aims

- To ensure the safeguarding of children within and beyond the school setting by detailing appropriate and acceptable uses of online technologies.
- To outline the roles and responsibilities of everyone.
- To have clarity about procedures following the misuse of any online technologies both within and beyond the school setting.
- To work with parents/carers and the wider community towards their appropriate input into policies and procedures and to maintain a continued awareness of both the benefits and potential issues of online technologies.

4. Roles and responsibilities of the school:

4.1 Roles: Governors, Headteacher and e-Safety Leader

It is the overall responsibility of the Headteacher and e-Safety Leader with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the Academy with specific responsibilities as follows:

- Headteacher is responsible for promoting e-Safety across the curriculum and have an awareness of how this is being developed, linking this to the school development plan.
- Headteacher has designated an e-Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe Computing/ICT learning environment.
- The headteacher will inform the Governors at Curriculum meetings about the progress of the e-Safety curriculum and ensure Governors know how this relates to child protection. At Full Governor meetings all Governors will be made aware of key e-Safety developments.
- The Governors MUST ensure Child Protection is covered with an awareness of e-Safety and be clear how it is being addressed within the Academy. It is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.

• An e-Safety Governor will, where necessary, challenge the e-Safety Leader about this AUP having appropriate strategies to clearly define the roles and responsibilities for the management, implementation and safe use of online technologies.

• These parties will jointly ensure that any misuse or incident is dealt with according to policy and appropriate action is taken, to extremes such as suspending a member of staff or involving the Police. See appendices for procedures on misuse.

4.2 Roles: e-Safety Leader

It is the role of the designated e-Safety Leader to:

• Liaise with the PSHE, Child Protection and Computing/ICT leads so that all policies and procedures are up-to-date to take account of any emerging issues and technologies.

• Provide up-to-date information for all staff to teach and manage e-Safety effectively. Time and resources will be provided for the e-Safety Leader and staff to be trained and to update policies as appropriate.

• Involve parents/carers so they feel informed and know where to go for advice.

• Ensure there is appropriate and up-to-date anti-virus and anti-spyware software on all susceptible devices and that this is reviewed and updated on a regular basis.

• Ensure that staff can check for viruses on devices including memory sticks and transferable data files to minimise issues of virus transfer.

• Ensure that filtering is set to the correct level for staff and children at the initial set up of all devices and on the learning platform (VLE).

• Ensure that all adults are aware of the filtering levels and why they are in place.

• Monitor the use of internal email.

• Report overuse of blanket emails or inappropriate tones to the headteacher.

• Have an overview of all Academy internet and online technology usage – it is the class teacher's responsibility to monitor such usage by the children in their class.

• Keep a log of incidents for analysis to help inform future development and safeguarding.

• Report issues and update the headteacher on a regular basis. This will be reported, as necessary, in the Governors.

• Ensure that the AUP is reviewed annually.

4.3 **Roles: Staff or adults at the Academy**

It is the responsibility of all staff/adults within the Academy to:

- Ensure that they know who the Designated Person for Child Protection is so that incidents which involve a child can be reported. Where an allegation is made against a member of staff it should be reported immediately to the headteacher. In the event of an allegation made against the headteacher, the Chair of Governors must be informed immediately.

- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed immediately.

- Report incidents of personally directed "bullying" or other inappropriate behaviour via digital technologies in the same way as for other non-physical assaults.

- Be up-to-date with e-Safety knowledge that is appropriate for the age group they work with and embed this throughout the curriculum.

- Ensure that children and young people are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner and know what to do in the event of an incident.

- Monitor pupil's choices of usernames on the learning platform (VLE).

- Respond promptly if a pupil believes their VLE password is known by others.

- Keep Academy information confidential and not breach the Data Protection Act.

- Not disclose security passwords or leave a device unattended when they are logged in.

- Follow security procedures if any data is required to be taken from the school premises.

- Use caution and measures such as installed anti-virus software to prevent the transfer of viruses to the school network from removable media and the internet.

- Report any accidental 'misuse' or access to inappropriate materials to the e-Safety Leader.

- Not use personal equipment such as digital cameras in school for work purposes. Any such use should be agreed or reported promptly to the e-Safety Leader or Headteacher.

- Not download or store any school personal data (including pupil photographs) at home.

- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.

- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff and adults – see appendix 1.

4.4 **Roles: Children**

Children will be:

- Involved in the review of our Acceptable Use Policy through the school council or other appropriate group, in line with this policy being reviewed and updated.

- Expected to follow the Internet Usage Agreement (see appendix 3) whilst within school.

- Taught to use the Internet in a safe and responsible manner through Computing/ICT, PSHE and across the curriculum.

- Taught to tell an adult about any inappropriate materials, contacts from someone they do not know or other issues straightaway.

4.5 **Roles: Parents/Carers**

We want our parents/carers to support the Internet Usage Agreement by signing it with their children (or for younger pupils for them) to confirm both pupil understanding and acceptance and so that it is clear that we are working together. It is intended that as guidance these rules extend to children when they use digital technologies outside of school.

We hope that parents/carers will work with us to update to our procedures and rules so that they best match any new technologies or issues as they arise.

5 . Appropriate use by staff or adults at the Academy

Staff members who have password protected access to the Academy network have this so that they can access and manage appropriate resources for the children they teach and other Academy work. Such staff also have access to a range of peripheral ICT equipment which is similarly supplied to appropriately resource their work.

All staff will receive a copy of this Policy, including the Acceptable Use Rules for Staff (appendix 1), which makes clear how the Academy's Digital resources should be used. An abridged version of the Rules will be given to adults who work in the Academy for short periods (appendix 5).

5.1 In the event of inappropriate use by staff or adults at the Academy

If a member of staff is believed to have deliberately misused any of the Academy's digital resources in any manner suspected to be inappropriate, a report must be made to the Head of School immediately.

Also see appendix 2 – 'Procedures Following Misuse by Staff' (this includes minor events and accidental misuse and has for a list of actions relating to the scale of the incident).

5. **Appropriate use by children**

The Internet Usage Agreement for pupils (appendix 3) details how children are expected to use the internet and other technologies within school and gives guidance for home usage. For example, knowing how to conduct research or write an email to another child.

The downloading of materials, for example music files or photographs needs to be appropriate and 'fit for purpose' e.g. based on research for work and be copyright issue free.

Children will be taught and encouraged to consider the implications for misusing the internet such as posting inappropriate materials to websites, as this can lead to legal implications.

In the event that a pupil accidentally accesses inappropriate materials the child should take appropriate action e.g. hide the screen or close the window and report this to an adult immediately.

Where a child or young person feels unable to disclose any issues or misuses against them to a trusted adult, they should have been made aware of the facilities such as the CEOP Report Abuse button (www.thinkuknow.co.uk) and Childline number (0800 1111) to seek advice and help.

The school council will be actively involved in discussing the acceptable and positive use of online technologies alongside the rules needed for this.

6.1 In the event of inappropriate use by children – 'internal'

The Academy will never blame a child for an accidental incident.

Should a child be found to have deliberately misused the school's online facilities the following consequences will occur:

- The parents/carers of the child will be contacted.
- A formal incident record will be made.
- Further or serious misuse of the rules will result in a suspension of internet access for a period of time and a letter will be sent to parents/carers (this would include any incident where a child is deemed to have misused technology against another child or adult).
- Depending on the seriousness of the incident other sanctions may be employed.

Also see appendix 4 – 'Procedures Following Pupil Misuse or Incident'

6.2 In the event of inappropriate use by children – 'external'

If the Academy becomes aware of an incident outside of school it will raise this with any parents/carers involved and offer guidance toward the resolution of the issue. In extreme cases some such situations may require the contacting of outside agencies.

7. The curriculum and tools for learning

7.1 Internet use

Children will be taught how to use online digital technologies safely and responsibly, for researching information, exploring concepts, deepening knowledge and communicating effectively in order to further learning. This will be through both Computing and PSHE lessons and across the curriculum. The following concepts, skills and competencies will be taught by the time pupils leave Year 6:

- internet literacy, including making good judgements about websites.
- understanding risks such as viruses and opening mail from a stranger.
- knowledge of copyright, plagiarism, file-sharing and downloading illegal content issues.
- data privacy awareness – knowing what is and is not safe to upload.
- how to access to appropriate guidance, where to go for advice and how to report abuse.

These skills and competencies will be taught within the curriculum so that children have the security to explore how online technologies can be used effectively and in a safe and responsible manner. Pupils will know how to deal with any incidents with confidence. Personal data safety – we will ensure that information uploaded to websites and otherwise placed in the public domain does not include pupil's personal information including their:

- full name (first name, sometimes with surname initial, is usually acceptable)
- address, telephone number or email address
- DoB

7.2 Email use

Via our managed Virtual Learning Environment (VLE) we provide email addresses for children to use. Pupil email accounts can only send and receive messages to other school email accounts. Any deviation from this for a specific project or purpose must be agreed with the e-Safety Leader.

Pupils will be taught what constitutes acceptable use of the email system and be aware how to report any misuse they may encounter.

Parents/carers are encouraged to monitor emails both sent and received.

7.3 Contributions to online communities

Staff approval is required before children make contributions to any external online community such as a forum, blog or wiki. Staff, in turn, must gain the approval of the e-Safety Leader before children participate in any externally controlled community including online chatrooms or webcam links.

7.4 Mobile phones and related technologies

Without the express permission of a staff member and agreement of e-Safety Leader the pupils use of mobile phones (or any device which can communicate independent of school networks) is not allowed in the Academy or its school grounds during the school day, at after-school clubs, or on a trip or residential visit. Pupils may leave mobile phones in the main school office for the day.

Staff should never use their personal phones to contact children and are discouraged from contacting parents/carers in this way.

8. Photographs and video

The term 'image' refers to the taking of photographs or video via any camera or other technology.

Academy images of children will not be in any way compromising or inappropriate. If a member of staff is unsure if a photograph is appropriate for publication they should seek guidance from the eSafety Leader or Headteacher.

Images should only reference a child's first name. Online filenames must not identify children. Where possible group photographs are preferable to those of individual children.

Images of children may only be uploaded online by staff or volunteers working under the direct supervision of staff if parents/carers have signed their permission for this (see appendix 3 - 'Pupil Rules and Parental Permissions').

Images may only be uploaded to the school's official platforms such as its website or social media platform.

Images of children should be stored securely on the school network, never on personal devices. The school will provide devices (e.g. iPads or cameras for this purpose).

A pupil's personal space on the Academy learning platform should not host any inappropriate images. It is highly recommended that parental/carer approval is required re. any home uploading.

Images used to identify children in any external online community should be representative of the child (e.g. an avatar or symbol) rather than photographic.

8.1 Photographs and video – Parents/Carers

Parents/carers are welcome to take photographs at Academy performances and events under the following terms and conditions:

- Photographs should primarily be of the parent/carer's own child/children.
- The photographs taken should be for personal/close family use only.
- Excepting 'prints' the photographs should not be published in any manner. This includes any website or social networking site publication.

The videoing of parent/carer's children may take place unless an issue such as performance copyright exists. The Academy will inform parents/carers prior to an event and at the start of each event if videoing is allowed. If videoing is permitted the conditions are as above for photography.

Outside of performances and events parents/carers are requested to ask a member of staff's permission before taking any photographs or videos at the Academy (conditions as above).

9. Filtering and safeguarding measures

Our YHGfL broadband connectivity has a strict filtering system to resist the delivery of inappropriate content. Anti-virus and spyware software is on our network and is updated on a regular basis. A professional firewall is used to protect our network, including all information about our children, from access by unauthorised users. Our wireless network has an encryption code to resist hacking.

Our learning platform has a 'Report Abuse' button. Children are taught the purpose of this both to protect themselves and others, links are made to similar buttons in external online communities.

10. Support

e-Safety teaching for pupils will take place at a classroom and key stage level on a termly basis. Updates for parents/carers will take place at least once a year and as new issues arise. Guidance and links to related websites will be provided via our website.

The school will help to provide access to the internet for parents/carers so that appropriate advice and information can be accessed where is no internet at home (subject to arrangement).

Appendices 1.

Acceptable Use Rules for Staff

To ensure that all adults within the Academy are aware of their responsibilities when using any online technologies they are asked to sign their agreement to specific Acceptable Use Rules. This is both to provide an example to children regarding safe and responsible use and as a safeguard from any potential allegations or inadvertent personal misuse.

These rules apply to all online usage and to anything that may be downloaded or printed.

General:

- I have been given a copy of the Acceptable Use Policy to refer to for all e-safety procedures I should follow.
- I know who the e-Safety Leader is.
- I will only use Academy equipment in an appropriate manner and for professional uses. (n.b. if portable equipment is taken home staff need to ensure their home insurance covers this).
- I will adhere to copyright and intellectual property rights.
- I know that I should not be using Academy systems for personal use unless this has been agreed by the e-Safety Leader or Head of School.
- I will take measures or seek advice to prevent the potential introduction of viruses to the network.
- I will ensure that I keep my passwords secure and try not to leave any machine 'logged in'.
- I will report any accidental misuse.
- I will report any incidents of concern to the e-Safety Leader or Head of School.

Photographs & video:

- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via email.
- I know that all Academy images should appropriate and beyond first names not reveal any personal information about children if uploaded to the internet.
- I should not use take images on any personal devices at the Academy. Any such use felt necessary should be agreed in advance or reported promptly to the e-Safety Leader or Head of School.
- Images of children should be stored securely on the school network, never on personal devices.

Communication & Social Networking:

- I will ensure all messages are written carefully and politely (emails can be forwarded to unintended readers).

- I realise that I am putting myself at risk of misinterpretation and allegation should I contact children via any systems other than Academy provided ones. I will not use any non-Academy online technologies to communicate with any current pupils. Specifically I will not accept or request the 'friendship' of pupils.

- I understand the value of setting my 'Privacy' settings appropriately on any social networking site and not stating my place of work – this will help to prevent unacceptable 'friendship' requests.

- I will not risk bringing the Academy into disrepute by discussing any aspect of my work or by making any Academy related comments or references online other than (as delegated) via our VLE and other official Academy web presence agreed protocols. I will solely use my Academy email address for work-related communications. Any variance from the above must be agreed with the e-Safety Leader or Headteacher.

- I have read, understood and agree with the Academy's 'Acceptable Use of Digital Technologies Online (e-Safety) Policy' and the rules specified above.

- I understand my responsibilities regarding safeguarding children when online technologies are used.

Signed: _____ Date: _____ Name (printed): _____

2. Procedures Following Staff Misuse or Incident

The Headteacher will ensure these procedures are followed, in the event of misuse or incident:

A. An inappropriate website is accessed accidentally: Report incident /website to the e-Safety Leader. e-Safety Leader to log and contact the IT helpdesk filtering service.

B. An inappropriate website is accessed deliberately: Ensure that no one else can access the material by switching off display. If possible preserve any evidence. Report to the e-Safety Leader and Head of School immediately. Contact Police or other agencies as necessary. Decide on appropriate disciplinary response. e-Safety Leader to log and inform the helpdesk filtering services as with A.

C. A staff member receives inappropriate material: Do not forward this material to anyone else – doing so could be an illegal activity. Alert the e-Safety Leader and Head of School

immediately. e-Safety Leader to preserve any evidence and log the nature of the material. Contact Police or other agencies as necessary.

D. A staff member has used ICT equipment inappropriately: Ensure that no one else can be affected by the activity. If possible preserve any evidence. Report to the e-Safety Leader and Head of School immediately. If involving children report to Designated Person for Child Protection follow Child Protection Policy and inform parents/carers. Contact Police or other agencies as necessary. Decide on appropriate disciplinary response.

E. A staff member has communicated with a child inappropriately: Ensure the child is reassured and remove them from the situation immediately. Report to the Head of School, Designated Person for Child Protection and e-Safety Leader. Preserve the information received by the child if possible. Head of School to follow the Allegation Procedure and/or Child Protection Policy. Notify parents/carers. Contact CEOP / Police as necessary. Decide on appropriate disciplinary response.

F. Inappropriate, damaging, malicious or threatening comments/files are posted online: Preserve any evidence. Support any individuals affected. Inform the e-Safety Leader and Head of School immediately. Investigate. Decide on appropriate remedial actions. Contact Police or other agencies as necessary. If posted by staff member decide on appropriate disciplinary response.

3. Pupil Rules and Parental Permissions

4. Procedures Following Pupil Misuse or Incident

The Headteacher will ensure these procedures are followed, in the event of misuse or incident:

A. An inappropriate website is accessed accidentally: Reassure the child that they are not to blame and praise them (or 'informant' peer) for being safe and responsible by telling an adult. Report incident /website to the e-Safety Leader. Decide if parents/carers need to be notified. e-Safety Leader to log and contact the IT helpdesk filtering service.

B. An inappropriate website is accessed deliberately: Refer the child to the Internet Usage Agreement. Report incident /website to the e-Safety Leader. Decide on appropriate sanction. Notify parents/carers. e-Safety Leader to log and contact the IT helpdesk filtering service.

C. A child has received an inappropriate communication: Ensure the child is reassured and remove them from the situation immediately. Preserve the communication/all related evidence as received by the child. Report to the Head of School, Designated Person for Child Protection and e-Safety Leader. Follow the Child Protection Policy. Contact CEOP / Police as necessary. Notify parents/carers.

D. Inappropriate, upsetting, malicious or threatening comments/files are posted online: Preserve all related evidence. Support any individuals affected. Report to the Head of School, Designated Person for Child Protection and e-Safety Leader. Decide on appropriate remedial actions. If posted by a child decide on appropriate sanctions. Notify parents/carers.

N.B. There are three events which must be reported directly to the police:

- Indecent images of children found.
- The sending of obscene materials to a child.
- Suspicion of 'grooming' behaviour.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if such an event occurs. If in doubt, do not power down the machine.

It is important to remember that any offensive images that may be encountered should never be forwarded to anyone else - even if it is to report them as illegal, as the forwarding itself may constitute illegal activity and could bring liability to prosecution and investigation by the police.

6. **Acceptable Use Rules for Staff (abridged version for short-term work)**

To ensure that all adults within the Academy are aware of their responsibilities when using any online technologies they are asked to sign their agreement to specific Acceptable Use Rules. This is both to provide an example to children regarding safe and responsible use and as a safeguard from any potential allegations or inadvertent personal misuse.

These rules apply to all online usage and to anything that may be downloaded or printed. General:

- I will only use Academy equipment in an appropriate manner and for professional uses.
- I will adhere to copyright and intellectual property rights.
- I know that I should not be using Academy systems for personal use unless this has been agreed by a Senior Manager.
- I will take measures or seek advice to prevent the potential introduction of viruses to the network.
- I will ensure that I keep all passwords secure and try not to leave any machine ‘logged in’.
- I will report any accidental misuse.
- I will report any incidents of concern a Senior Manager. Photographs & video:

- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via email.

- I know that all Academy images should appropriate and beyond first names not reveal any personal information about children if uploaded to the internet.

- I should not use take images on any personal devices at the Academy.

- Images of children should be stored securely on the school network, never on personal devices.

Communication & Social Networking:

- I realise that I am putting myself at risk of misinterpretation and allegation should I contact children via any systems other than Academy provided ones. I will not use any non-Academy online technologies to communicate with any current pupils. Specifically I will not accept or request the 'friendship' of pupils.

- I understand the value of setting my 'Privacy' settings appropriately on any social networking site and not stating my place of work – this will help to prevent unacceptable 'friendship' requests.

- I will not risk bringing the Academy into disrepute by discussing any aspect of my work or by making any Academy related comments or references online.

- I have read, understood and agree with the Academy's 'Acceptable Use of Digital Technologies Online (e-Safety) Policy' and the rules specified above.

- I understand my responsibilities regarding safeguarding children when online technologies are used.

Signed: _____ Date: _____ Name (printed): _____