ONLINE SAFETY POLICY

SCHOOL: TARLETON COMMUNITY PRIMARY SCHOOL

Key Personnel

Name	Role
James Glaister	Online Safety Champion
Mike Adams	Online Safety Governor
Chris Upton	Headteacher/Lead DSL
Janette Higson	Deputy Headteacher/Back up DSL/ Website Co-ordinator

Our Vision for Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Lancashire Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.
- Using tablet technologies safely and effectively to support the school's mission statement and enhance learning across the curriculum in a safe and responsible way.
- Have a rigorous reporting procedure for Online Safety related incidents.
- Each year group has a Computing unit focussed on Online Safety each year delivered at an appropriate level. Assemblies are also held when Online Safety issues are tackled and discussed with the children.

OFSTED's three main areas of Online Safety risk:

- Content: children need to be taught that not all content is from a reliable source.
  Examples: inappropriate content, lifestyle websites (e.g. self-harm, anorexia etc.) ignoring age ratings in games, substance abuse etc.

- Contact: children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.
  Examples: grooming, online bullying, identity theft including "frape" and sharing passwords.

- Conduct: Children need to be aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves or others.
  Examples: privacy issues including the disclosure of personal information, health and wellbeing i.e. the amount of time spent online, sexting, copyright law.

School Online Safety Policy

The school is aware that all staff need to be involved in keeping children safe when using technology. However an Online Safety Champion has been appointed as the main point of contact for Online Safety related issues and incidents.

The roles & responsibilities of the Online Safety Champion:

- Operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents including AUPs.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety issue occur.
- Ensuring an Online Safety log is appropriately maintained and regularly reviewed.
- Keeping up-to-date with Online Safety issues and guidance through liaison with the L.A. and advice given through agencies such as the Child Exploitation and Online Protection Centre (CEOP)
- Providing/arranging Online Safety advice/training for staff/governors/parents.
- Liaising closely with the DSP or CPO to ensure a coordinated approach across relevant safeguarding areas.
- Liaising with the British Values lead person on preventing extremism through safe practise of Computing.

Our Online Safety Policy has been written by the school, building on Government guidance. It has been agreed by the senior leadership team and approved by governors.

The Online Safety Policy will be reviewed annually. This policy will next be reviewed in Spring 2018.

Mobile phones

Children:

- Children are forbidden from having mobile phones on their person whilst on school premises.
- Children must hand their mobile phones to the school office upon arrival at school and it is their responsibility to retrieve them at the end of the school day.
- The phone must be switched off and only switched on again when the child has left the school grounds.

Staff:

- Personal mobile phones belonging to members of staff must be switched off for the duration of the school day unless they are being used in the Staffroom or Office areas.
- Staff are permitted to have their mobile phone on their person – in a pocket or bag but they must be switched off in the school (with the exception of Staffroom and Office areas) within school hours.
- Staff must not access their mobile phone when children are present in the room.
- No images, video or audio of children is to be recorded on personal mobile phones without explicit permission being given by the head teacher.
- Staff may access the school's Wi-Fi on their mobile phone but for work purposes only.

Use of digital media (cameras and recording devices)

Staff:

- The school has access to and use of a range of digital cameras and LearnPad tablets. The cameras and the memory cards within them are forbidden from being taken off the premises by any member of staff unless explicit permission is given by the head teacher or the adult is a designated person.
- The only exception to the above rule is that children's headshots for use in reports may be taken home for the purposes of being included in the children's reports once completed.
- LearnPads come under the same restrictions as the digital cameras.
- Written permission is obtained once per academic year from parents for photographs of their children to be taken and used. New arrivals are presented with the same permission form.
- Written permission has been obtained for adults working within school to have their photographs taken and used.
- Staff are given a list at the start of the academic year of children whose parents have not given permission for their photographs to be used on the school website, social media, newspaper articles or publically visible displays.
- All staff members employed by the school have permission to take images/video/audio of the children in school but not on personal recording equipment as stated in the Mobile phone usage section of this document.

Parents:

- Parents are permitted to take photographs of their own children on school premises on the provision that the photographs are for their own use.
- Parents are aware that taking a photograph that includes other children could constitute a potential breach of Data Protection legislation.
- If parents want to take a photograph/video that includes other children then they need to obtain permission from the parents of the other children.
- Parents are aware that uploading images/video of their child alongside other children to social network sites is not acceptable unless specific permission has been obtained from the parents of the other children.

Storage of photographs/video

- Any storage of photographs/video or audio of children or staff on school devices is to occur on the school server or password protected cloud account.
- No photographs/video or audio of children is to be stored on removable USB drives unless the drives are being kept securely on school premises, reports must be saved onto the school server, not USB. (NB staff may take the

Tempest photographs of the children home on USB to work on reports but they should be deleted after reports are saved onto the server.)

- LearnPads are able to upload digital media to cloud storage which is password protected.
- Staff are not to remove school cameras or LearnPads containing photographs/video or audio of children from the school premises except for designated persons for designated purposes.
- Once children's images have been used for display they need to be disposed of by shredding in the office.
- In the event of a third party taking photographs of the children e.g. newspaper, written permission should be obtained from the parents of the children informing them of the way in which their child's image will be used.

e-mail

- All staff have access to BT Lancashire Outlook system for work-based e-mail.
- Staff are permitted to access their personal e-mail accounts on school premises on personal and school equipment at playtimes, lunchtimes or at other times when no children are present.
- Only official e-mail accounts or password protected staff-designated e-mail accounts are to be used for professional communication.
- Any incidents of SPAM on official e-mail accounts should be reported to the Online Safety Champion.
- All e-mails must be sent with the e-mail disclaimer at the bottom.

Social Networks

Staff:

- Staff are permitted to have social network accounts (Facebook, Twitter, Pinterest etc.) but it is not acceptable to post content that:
  brings the school into disrepute;
  leads to valid parental complaints;
  is deemed as derogatory towards the school and/or its employees;
  is deemed as derogatory towards pupils, parents or carers;
  brings into question their appropriateness to work with children and young people.
- All staff social media accounts must be private and not open to public scrutiny. If staff are unsure as to whether their social media is private they should consult with the Online Safety Champion.
- It is not acceptable for staff to accept friend/follower requests from students who are currently enrolled at the school unless they are family members.
- Communication with past pupils, parents or siblings of pupils (not enrolled at school) is strongly discouraged particularly if the pupils are under the age of 18 years of age.
- In the case of incidents on social media (outside of school hours) affecting children's behaviour or causing issues during school hours then a meeting will be arranged with the Child Protection Officer, Online Safety Champion, the child who has committed the incident and the child's parents to deal with the "spill over" into school hours.

Parents:

- Parents should be aware that posting inappropriate comments about individual members of staff or children can be construed as online bullying. If

this situation arises then the parent(s) in question will be invited into school to discuss their issues and asked to remove the offending post.

- It is not acceptable for parents to discuss issues that they may be experiencing at school on social media as it may bring the school into disrepute. It is preferred that the parents in question make an appointment with the relevant staff member so that their issue can be dealt with directly and then the offending post deleted.
- As stated previously; parents are aware that uploading images/video of their child alongside other children to social network sites is not acceptable unless specific permission has been obtained from the parents of the other children.
- Parents are aware that the legal age requirement for children to have social media profiles is 13 years of age. If they choose to allow their child to have a social media profile under this age then they are causing the social media network in question to break the law.

Preventing Extremism

The school is aware that it has a role to play to prevent radicalisation and extremism. To prevent the radicalisation of young people the school:

- Has a filtering system to block out inappropriate websites.
- A reporting system in place for both staff and pupils to keep a record of any incidents which occur.
- Has received training on awareness and prevention of extremism. (FBV)
- Has AUPs in place for staff, governors, parents and children.
- Is teaching Fundamental British Values as part of the school curriculum (see planning)
- Through Online Safety, teaches the children to become critical learner and so they know what is acceptable or unacceptable even though filters are in place.

School Website

- The Deputy Head is the designated persons responsible for the school website.
- The designated person is aware of the information that should be included on the school website according to the School Information Regulations (Amendment) 2012.
- It is the designated persons' responsibility to ensure the information on the school website is kept up-to-date.
- Downloadable materials are to be made accessible in .pdf format only, to prevent the content being manipulated and redistributed without school's knowledge or consent.

Infrastructure & Technology

In order to keep children safe, the school subscribes to the Lancashire Grid for Learning so internet filtering is provided by default.
Sophos Antivirus software is installed and configured on all necessary devices to protect from online viruses.

Access

- When accessing school equipment and online materials children are supervised by a trusted adult and protected by the online filtering system.
- Children's accounts for the server restrict their access to certain areas of the network.
- Access to confidential data is restricted to the school office e.g. SIMS etc.
- Staff members have access to all school systems as required.
- All users of the school network have a secure username and password.
- The administrator password for the school network is available to the school technician, bursar, Deputy Head and Computing coordinator. It is stored in a safe location.

Managing the network and technical support

- All servers, wireless systems and cabling are securely located and access is restricted.
- Critical updates and software installation involving executable files is completed by the school technician who visits fortnightly.
- Security breaches should be reported to the Online Safety Champion.

Dealing with incidents

Illegal offences:

- Any suspected illegal material or activity must be reported to the head teacher immediately who must refer this to the relevant external authority.
- Illegal content must be reported to the Internet Watch Foundation who have a licence to investigate, **schools do not.**
- Details of what constitutes illegal offences can be found at http://iwf.org.uk

Inappropriate use (a copy to be provided to each classroom and Computing Suite)

<table>
<tr><th>Incident</th><th>Procedure & Sanction</th></tr>
<tr><td>Accidental access to inappropriate materials.</td><td rowspan="4">Minimise the webpage/turn off the monitor.
Tell a trusted adult.
Enter the details in the Incident Log and report to LGfl filtering services if necessary.</td></tr>
<tr><td>Using other people's logins and passwords maliciously.</td></tr>
<tr><td>Deliberate searching for inappropriate materials.</td></tr>
<tr><td>Bringing inappropriate electronic files from home.</td></tr>
<tr><td></td><td>Inform the Online Safety Champion.
Enter the details in the incident log.
Additional awareness raising Online Safety issues and the AUP with individual child/class.
More serious or persistent offences may result in further disciplinary action in line with the Behaviour Policy.
Consider parent/carer involvement.</td></tr>
</table>

The team responsible for dealing with Online Safety incidents is (any combination of):

The Online Safety Champion;
Computing Coordinator;
Child Protection Officer;
Designated Online Safeguarding Governor
Head Teacher.

Acceptable Use Policies

- See Appendices for AUPs for Staff/Governors, Students/Supply Teachers and children.
- Also attached are letter templates for events e.g. Christmas productions where parents must give consent for their child's image to be included in other parents' photographs.

Appendices

Appendix 1: Acceptable Use Policy for children including letter for parents.

Appendix 2: Acceptable Use Policy for staff and goverors.

Appendix 3: Acceptable Use Policy for students and supply teachers.

Appendix 4: child-friendly Online Safety rules

Appendix 5: permission letter for school plays and other events.

Appendix 6: inappropriate use of digital technologies report form.

Appendix 7: Staff Information Systems Code of Conduct.

Reviewed: Autumn 2017

To be reviewed: Spring 2019

Date Approved: _____

Signed: _____

Appendix 1

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- ✓ I will only use the Internet and/or online tools when a trusted adult is present.
- ✓ I will only use my class e-mail address or my own school email address when emailing.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- ✓ I will not deliberately bring in inappropriate electronic materials from home.
- ✓ I will not deliberately look for, or access inappropriate websites.
- ✓ If I accidentally find anything inappropriate I will tell my teacher immediately.
- ✓ I will only communicate online with people a trusted adult has approved.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not give out my own, or others', details such as names, phone numbers or home addresses.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will not arrange to meet anyone that I have met online.
- ✓ I will only open/delete my own files.
- ✓ I will not attempt to download or install anything on to the school network without permission.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety.
- ✓ I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

We have discussed this Acceptable Use Policy and

…….. [Print child's name] agrees to follow the Online Safety rules and to support the safe use of ICT at *Tarleton Community Primary School*

Parent /Carer Name (Print) ……

Parent /Carer (Signature) …… ……..

Class …… Date……

This AUP must be signed and returned before any access to school systems is allowed.

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School Online Safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing Online Safety as part of your child's learning, we will also be holding Parental Online Safety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about Online Safety for parents and carers, please visit the Lancsngfl Online Safety website http://www.lancsngfl.ac.uk/Online Safety

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact Mr Glaister.

Yours sincerely,

Chris Upton
Headteacher

Appendix 2

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of *<insert name>.*
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……..

Full Name ……..……(PRINT)

Position/Role ……

Appendix 3

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will respect copyright and intellectual property rights.
4. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
5. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
6. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
7. I will not install any hardware or software onto any school system.
8. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature
I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature
……..

Date
……

Full Name
……(PRINT)

Position/Role
……

Appendix 4

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

Online Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.

Appendix 5

Dear Parent/ Carer,

Your child will be appearing in <> on <>. We are aware that these events are special for children and their relatives / friends and form treasured memories of their time at school.

We have a rigorous policy in place with regard to taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images / video being used in general circumstances.

Many parents / carers like to take photographs / videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the pictures. In these circumstances, we request specific consent for images / videos to be taken by a third party (i.e. other parents). We need to have permission from all parents / carers of children involved in the production to ensure that they are happy for group images / videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images / videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook without the specific permission of the individuals included in the footage.

These decisions are not taken lightly, but we have to consider the safeguarding of all our children and respect parents' rights to privacy.

Yours sincerely,

Chris Upton
Headteacher

Child's name: _____ Date: _____

I agree / do not agree to photographs / videos being taken by third parties during <> on <>

Signed _____ *(Parent / Carer)*

Print name _____

Appendix 6

Date:
Time:
Class:
Adult:
Nature of incident: (e.g. inappropriate content accessed, unauthorised photographs being taken, Online Safety policy not being adhered to etc.)
Action taken:

Appendix 7

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school Online Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.
Signed: …… Capitals: …… Date: ……
Accepted for school: ……