



# **Acceptable Use Policies for Education Settings and their Wider Communities**

**for Children, Young People, Parents/Carers, Staff, Volunteers, Visitors and other Community Members**

Date of issue:	May 2019
Review Date	May 2020
To be reviewed	Headteacher, Staff and Governors
Authorised by	Headteacher and Governors



New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

**This Acceptable Use Policy is intended to ensure:**

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Page taken from  
<https://swgfl.org.uk/assets/documents/appendix-staff-volunteer-aea.docx>



# Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation / KS1)

**This is how we stay safe when we use computers:**

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen or if I feel worried or unhappy
- I only click on links and buttons when I know what they do
- I keep my personal information and passwords safe online
- I only send messages online that are polite and friendly
- I know that if I break the rules, I will be given a warning by my teacher and might not be allowed to use a computer / tablet

Signed (child): .....

Signed (parent): .....

# Early Years and KS1 Acceptable Use Poster

**Be**

**SAFE**

**Online**

- 1** I only go online with a grown up
- 2** I am kind online
- 3** I keep information about me safe
- 4** I tell a grown up if something online makes me unhappy

**eis Kent**  
Education IT Services

**Kent County Council**  
kent.gov.uk

Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk



# Pupil Acceptable Use Agreement – for KS2 pupils

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

## **This Acceptable Use Agreement is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk
- that young people will have good access to digital technologies to enhance their learning and in return, the pupils agree to be responsible users.

## **Acceptable Use Policy Agreement**

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

### **For my own personal safety:**

- I understand that the Holy Trinity Academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details.)
- I know that people I may meet online may not be who they way they are. If someone online suggests meeting up, I will immediately talk to an adult.
- I will immediately minimise and then report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

## **I understand that everyone has equal rights to use technology as a resource and:**

- I understand that Holy Trinity Academy's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

## **I will act as I expect others to act toward me:**

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite, friendly and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or share images of anyone without their permission.

## **I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:**

- Mobile devices should be kept in the academy office, switched off. I will only use it in school time if I have permission. I understand that, if I do use my own devices in the school time, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- If I notice and damage or faults involving equipment or software I will report it immediately.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites during school time.
- When using the internet for research or recreation, I recognise that:
  - I should ensure that I have permission to use the original work of others in my own work
  - Where work is protected by copyright, I will not try to download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful.

**I understand that I am responsible for my actions, both in and out of school:**

- I understand that the Holy Trinity Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I do not follow the rules then I will be given a warning by the class teacher or lose access to the school network / internet. Parents may be contacted and in the event of illegal activities the police will be contacted.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.**



## Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

I have read and understand the above and agree to follow these guidelines when:

- I use Holy Trinity Academy systems and devices
- I use my own equipment out of the academy in a way that is related to me being a member of this academy e.g. communicating with other members of the school, WhatsApp groups, social media accounts.

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

### Parent / Carer Countersignature

# KS2 Acceptable Use Poster

30 Winner! You were safe online

29

28

27

26 I will keep information about me and my passwords secret.

21

22

23 I will not be unkind to anyone online.

24

25 I acted unsafely online!

20 If someone asks me to meet them, I will always talk to an adult straight away.

19

18 I know that people online are strangers and they may not be who they say they are.

17

16 I acted unsafely online!

11 I always talk to an adult if I see something online which worries me.

12

13

14 I know there are laws that stop me copying online content.

15

10 I acted unsafely online!

9

8 I know I must only open messages online that are safe. If I am unsure I will ask an adult first.

7

6 I always check if information online is true.

1 Online

2

3 I ask an adult which websites I can look at or use.

4

5

**STAY SAFE Online**



Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk

## Statements for Children with Special Educational Needs and Disabilities

(These statements are based on ability levels rather than age)

### Children and Young People functioning at Levels P4 –P7

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see something I don't like online I tell a grown up
- I know that if I do not follow the school rules then **I will be given a warning by the class teacher**

### Children functioning at Levels P7-L1 (Based on Childnet's SMART Rules: [www.childnet.com](http://www.childnet.com) )

#### Safe

- I ask a grown up if I want to use the computer
- On the internet I don't tell strangers my name
- I know that if I do not follow the school rules then **I will be given a warning by the class teacher**

#### Meeting

- I tell a grown up if I want to talk on the internet

#### Accepting

- I don't open emails from strangers

#### Reliable

- I make good choices on the computer

#### Tell

- I use kind words on the internet
- If I see something I don't like then I tell a grown up

### Children and Young People functioning at Levels L2-4 (Based on SMART Rules: [www.childnet.com](http://www.childnet.com))

#### Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the school rules then **I will be given a warning by the class teacher**

#### Meeting

- I tell an adult if I want to talk to people on the internet
- If I meet someone online I talk to an adult

#### Accepting

- I don't open messages from strangers
- I check web links to make sure they are safe

#### Reliable

- I make good choices on the internet
- I check the information I see online

#### Tell

- I use kind words on the internet
- If someone is mean online then I don't reply, I save the message and show an adult
- If I see something online I don't like then I tell an adult



## Parent/Carers Acceptable Use Policy Statements

I have read and discussed the Acceptable Use Policy (attached) with my child

- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using the academy equipment may be monitored for safety and security reasons and to safeguard both my child and the school's systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the academy will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
- I understand that if the academy has any concerns about my child's safety online, either at the academy or at home, then I will be contacted
- I understand that if my child does not abide by the academy's Acceptable Use Policy then sanctions will be applied in line with the schools behaviour and anti-bullying policy. If the school believes that my child has committed a criminal offence then the Police will be contacted
- I, together with my child, will support the academy's approach to online safety (e-Safety) and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the academy's community
- I know that I can speak to the academy's Online Safety (e-Safety) Leader and The Computing Subject Leader (Mrs Innes), my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety)

I will visit the website (<http://holytrinitycalne.co.uk/>) for more information about the academy's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home

- I will visit [www.thinkuknow.co.uk/parents](http://www.thinkuknow.co.uk/parents), [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety), [www.internetmatters.org](http://www.internetmatters.org), [www.saferinternet.org.uk](http://www.saferinternet.org.uk) and [www.childnet.com](http://www.childnet.com) for more information about keeping my child(ren) safe online
- I will support the academy and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home

### I have read the Parent Acceptable Use Policy.

Child's Name..... Class.....

Parents Name.....Parents Signature.....

Date.....



# Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for pupils / students. Cloud systems such as Google Apps for Education services [www.google.com/apps/intl/en/terms/education\\_terms.html](http://www.google.com/apps/intl/en/terms/education_terms.html) may require that schools obtain 'verifiable parental consent' for children to be able to use the system and services. Schools may wish to incorporate this into their standard acceptable use consent forms. Schools will need to review and amend the section below, depending on which cloud hosted services are used. The Department for Education has published advice and information regarding Cloud (educational apps) software services and the Data Protection Act here: <https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act>

The school uses Google Apps for Education for pupils and staff. This consent form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupils and hosted by Google as part of the school's online presence in Google Apps for Education (**amend as appropriate as not all schools will use all options/apps**):

- **Mail** - an individual email account for school use managed by the school
- **Calendar** - an individual calendar providing the ability to organize schedules, daily activities, and assignments
- **Docs** - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office
- **Sites** - an individual and collaborative website creation tool

Using these tools, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

## Use of Cloud Storage Systems – Parental Consent

Child's Name..... Class.....

Parents Name.....

Parents Signature.....

Date.....

*Optional Form.*

This form was originally created and has been kindly shared by the South West Grid for Learning: [www.swgfl.org.uk](http://www.swgfl.org.uk)

This form should be used in accordance with DfE Guidance: <https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act>

## Letter for parents/carers

Dear Parent/Carer

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to: Laptops, iPads and other digital devices

- Internet which may include search engines and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphone's

Holy Trinity Academy recognises the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online safety (e-Safety) policies and procedures alongside the schools safeguarding measures.

Holy Trinity Academy takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. We employ rigorous systems for filtering using RM SafetyNet. However no system can be guaranteed to be 100% safe and the academy cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the schools internet and ICT facilities.

Full details of the academy's Acceptable Use Policy and online safety (e-Safety) policy are available on the school website (<http://holytrinitycalne.co.uk/>) or on request.

We request that all parents/carers support the schools approach to online safety (e-Safety) by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the academy's website's (<http://holytrinitycalne.co.uk/>) for more information about the school's approach to online safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk), [www.childnet.com](http://www.childnet.com), [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety), [www.saferinternet.org.uk](http://www.saferinternet.org.uk) and [www.internetmatters.org](http://www.internetmatters.org) for more information about keeping children safe online

Whilst the school monitors and manages technology use in school we believe that children themselves have an important role in developing responsible online behaviours. In order to support the academy in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and that you and your child discuss the content and return the attached slip. Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact the school online safety Leader and the Computing Subject Leader (Mrs Innes).

### Early Years/KS1/SEN

We understand that your child is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

Yours sincerely,

Mr Shore  
Headteacher



## Parent/Carer Acceptable Use Policy Acknowledgement Form

### Pupil Acceptable Use Policy Holy Trinity CofE Academy Parental Acknowledgment

I, with my child, have read and discussed **Holy Trinity CofE Academy** school Pupil Acceptable Use Policy.

I am aware that any internet and computer use using school equipment may be monitored for safety and security reason to safeguard both my child and the academy's systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school will take all reasonable precautions to reduce and remove risks but cannot ultimately be held responsible for the content of materials accessed through the Internet.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child's safety.

I will inform the academy or other relevant organisations if I have concerns over my child's or other members of the academy's communities' safety online.

I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the schools e-Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

Child's Name..... Signed (if appropriate).....

Class..... Date.....

Parents Name.....Parents Signature.....

Date.....



# Letter for Staff

**Please note this letter does NOT replace a Staff AUP**

Dear

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be “private” and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers as “friends” on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Please use your work provided email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this then please speak to the Online safety (e-Safety) Coordinator and ICT subject leader (Mrs Innes) or the Designated Safeguarding Lead /Manager (Mr Shore).

Documents called “Cyberbullying: Supporting School Staff”, “Cyberbullying: advice for headteachers and school staff” and “Safer professional practise with technology” are available in the staffroom to help you consider how to protect yourself online. Please photocopy them if you want or download the documents directly from [www.childnet.com](http://www.childnet.com), [www.e-safety.org.uk](http://www.e-safety.org.uk) and [www.gov.uk/government/publications/preventing-and-tackling-bullying](http://www.gov.uk/government/publications/preventing-and-tackling-bullying). Staff can also visit or contact the Professional Online safety Helpline [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline) for more advice and information on online professional safety.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the academy's policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to your line manager or the Designated Safeguarding Lead (Mr Shore) if you have any queries or concerns regarding this.

Yours sincerely,

Headteacher

## **Additional content for staff regarding online participation on behalf the School**

The principles and guidelines below set out the standards of behaviour expected of you as an employee of the school. If you are participating in online activity as part of your capacity as an employee of the academy then we request that you:

- Be professional and remember that you are an ambassador for the academy. Disclose your position but always make it clear that you do not necessarily speak on behalf of the academy.
- Be responsible and honest at all times and consider how the information you are publishing could be perceived
- Be credible, accurate, fair and thorough.
- Always act within the legal frameworks you would adhere to within academy, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Be accountable and do not disclose information, make commitments or engage in activities on behalf of the academy unless you are authorised to do so.
- Always inform your line manager, the designated safeguarding lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.

# Staff Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

**This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the academy's ethos, other appropriate academy policies, relevant national and local guidance and expectations, and the Law.**

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.
2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
5. I will not keep password info in plain sight.
6. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
7. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the academy. Any images or videos of pupils will only be used as stated in the academy's Image Use Policy and will always take into account parental consent. If images are taken off the academy site they should be encrypted using software such as Bitlocker or SafeHouse.
8. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment or via VPN. I will protect the devices in my care from unapproved access or theft.
9. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

10. I will respect copyright and intellectual property rights.
11. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
12. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Mr Shore) and/or the Online Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Designated Safeguarding Lead (Mr Shore) and/or the Online Safety Coordinator (Mrs Innes) and/or the designated lead for filtering (Andy Whittock) as soon as possible.
13. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged, stolen or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support lead (Mrs Innes) as soon as possible.
14. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.
15. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.
16. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
17. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
18. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Mr Shore) and/or the Online Safety Coordinator and ICT Subject Leader (Mrs Innes) or the Head Teacher.
19. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
20. *The academy may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the academy's information system or unacceptable or inappropriate behaviour may be taking place, the academy will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.*

**I have read and understood and agree to comply with the Staff Acceptable Use Policy.**

Signed: ..... Print Name: ..... Date: .....

Accepted by: ..... Print Name: .....



# Visitor/Volunteer Acceptable Use Policy

*For visitors/volunteers and staff who do not access school ICT systems*

***As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.***

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
2. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
3. I will follow the academy's policy regarding confidentiality, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via academy approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.
5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law
6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
8. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Mr Shore) or the Head Teacher.
9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Mr Shore) as soon as possible.

**I have read and understood and agree to comply with the Visitor /Volunteer Acceptable Use Policy.**

Signed: ..... Print Name: ..... Date: .....

Accepted by: ..... Date: .....



## Wi-Fi Acceptable Use Policy

### For those using school Wi-Fi

*Schools/settings may wish to use a paper or electronic AUP for guest access of Wi-Fi by members of the community. Schools may choose to require that visitors agree to an on screen electronic AUP as part of the process of accessing the Wi-Fi. This template is provided for schools to adapt and use as appropriate.*

***As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.***

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

The school provides Wi-Fi for the school community and allows access for the academy community and guests.

The use of ICT devices falls under Holy Trinity Academy's Acceptable Use Policy, Online safety Policy, Secure Data Handling Policy, Mobile Phone Policy and Behaviour Policy which all students/staff/visitors and volunteers must agree to, and comply with.

1. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
2. School owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I will take all practical steps necessary to make sure that any equipment connected to the school's service is adequately secure (such as up-to-date anti-virus software, systems updates).
4. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorised use or access into my computer or device.
5. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other

Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

6. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.
7. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
8. I will not attempt to bypass any of the schools security and filtering systems or download any unauthorised software or applications.
9. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
10. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
11. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Graham Shore), the Online Safety (e-Safety) Coordinator (Carey Innes), Computing Subject Leader (Carey Innes) and/or the designated lead for filtering (Andy Whittick) as soon as possible.
12. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online safety (e-Safety) Coordinator (Carey Innes), Computing Subject Leader (Carey Innes) or the Head Teacher.
13. I understand that my use of the schools Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the academy suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the academy terminate or restrict usage. If the academy suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

**I have read and understood and agree to comply with Holy Trinity Academy's Wi-Fi Acceptable Use Policy.**

Signed: ..... Print Name: ..... Date: .....

Accepted by: ..... Print Name: .....



# Social Networking Acceptable Use Policy

*For parents/volunteers running school/setting social media accounts e.g. PTA groups and committees*

1. As part of the academy’s drive to encourage safe and appropriate behaviour in the use of today’s technology, I will support the academy’s approach to online safety (e-Safety). I am aware that a public and global communication tool and that any content posted on the **Facebook page or WhatsApp group** may reflect on the school, its reputation and services. I will not use the **page or group** to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.
2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead (Mr Shore) or the head teacher. The head teacher (**or other appropriate member of senior leadership**) retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of **Facebook, or WhatsApp** or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. I will follow the school’s policy regarding confidentially and data protection/use of images. I will ensure that I have written permission from parents/carers or the school before using any images or videos which include members of the school community. Images of pupils will be taken on school equipment by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school and these will be for the sole purpose of inclusion on **Facebook**, and will not be forwarded to any other person or organisation.
5. I will promote online safety in the use of **Facebook and WhatsApp**) and will help to develop a responsible attitude to safety online and to the content that is accessed or created.
6. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account. The school Designated Safeguarding Lead and/or school management team will have full admin rights to the account.
7. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.
8. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead (Mr Shore) and/or head teacher immediately.
9. I will ensure that the Facebook page, or WhatsApp groups are moderated on a regular basis as agreed with the Designated Safeguarding Lead (Mr Shore) and/or head teacher.
10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.
11. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead (Mr Shore) or the head teacher.

I have read and understood and agree to comply with the School Parent Association Social Networking Acceptable Use policy.

Signed: ..... Print Name: ..... Date: .....



# Staff Social Networking Acceptable Use Policy

*For use with staff running official school social media accounts*

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to Online safety (e-Safety). I am aware that Facebook is a public and global communication tool and that any content posted may reflect on the school, its reputation and services. I will not use the site to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.
2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead (Mr Shore) and/or the head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school.
3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. I will follow the school's policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school. These will be for the sole purpose of inclusion on Facebook and will not be forwarded to any other person or organisation.
5. I will promote online safety (e-Safety) in the use of Facebook and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by a member of senior leadership team/ Designated Safeguarding Lead/head teacher prior to use.
6. I will set up a specific account/profile using a school provided email address to administrate the Facebook page and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Designated Safeguarding Lead and/or school leadership team/head teacher will have full admin rights to the Facebook page.
7. Where it believes unauthorised and/or inappropriate use of Facebook or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.
9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the head teacher and/or Designated Safeguarding Lead urgently.
10. I will ensure that the Facebook page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.
11. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.
12. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead (Mr Shore) or the head teacher.

I have read and understood and agree to comply with the School Social Networking Acceptable Use policy.

Signed: ..... Print Name: ..... Date: .....

Accepted by: ..... Print Name: .....