St. Joseph's

Catholic Primary School

Online Safety Policy

Safeguarding pupils, staff and school in a digital world

September 2024

CONTENTS

- Introduction
- Responsibilities of the School Community
- Learning and Teaching
- Parents and carers
- Managing and safeguarding ICT Systems
- Using the Internet; email; publishing content online; using images, video & sound; using video conferencing and other online text or video meetings; using mobile phones; using other technologies
- Protecting school data and information
- Dealing with Online Safety incidents including 'sexting'
- Reference to related documents

Introduction

This Online Safety policy recognises our commitment to Online Safety and acknowledges its part in the school's overall Safeguarding policies and procedures.

We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The Online Safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to Online Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets. We have adopted the good practice requirements for all staff which are included in the Lancashire Information Security Guidance document.

N.B. for the purposes of clarity and consistency throughout this document the person in school who is taking a lead on Online Safety is called the Online Safety coordinator**.**

The person in school taking on the role of Online Safety coordinator is Mrs Cunliffe
The following groups were consulted during the creation of this Online Safety policy: staff and governors

Responsibilities of the School Community

We believe that Online Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Management Team accepts the following responsibilities:

- Identify a person (the Online Safety coordinator) (or team) to take responsibility for Online Safety and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the Governors
- Develop and promote an Online Safety culture within the school community
- Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have Online Safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to Online Safety
- Receive and regularly review Online Safety incident logs; ensure that the correct procedures are followed should an Online Safety incident occur in school and review incidents to see if further action is required
- Take ultimate responsibility for the Online Safety of the school community

Responsibilities of the Online Safety Coordinator

- Promote an awareness and commitment to Online Safety throughout the school
- Be the first point of contact in school on all Online Safety matters
- Lead the school Online Safety team
- Create and maintain Online Safety policies and procedures
- Develop an understanding of current Online Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in Online Safety issues
- Ensure that Online Safety education is embedded across the curriculum
- Ensure that Online Safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff. who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy
- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- Monitor and report on Online Safety issues to the Online Safety group, the Leadership team and Governors as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Ensure an Online Safety incident log is kept up-to-date
- Ensure that Good Practice Guides for Online Safety are displayed in classrooms and around the school

Responsibilities of all Staff

- Read, understand and help promote the school's Online Safety policies and guidance
- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current Online Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Embed Online Safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all Online Safety incidents which occur in the appropriate log and/or to their line manager
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Additional Responsibilities of Technical Staff

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any Online Safety-related issues that come to their attention to the Online Safety coordinator and/or leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment
- Liaise with the Local Authority and others on Online Safety issues

Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance
- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Keep passwords private and do not share personal details.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all Online Safety incidents to appropriate members of staff
- Discuss Online Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting Online Safety
- Read, understand and promote the pupil AUP with their children
- Discuss Online Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's Online Safety policies and guidance as part of the schools overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in Online Safety awareness
- Ensure appropriate funding and resources are available for the school to implement their Online Safety strategy

Responsibility of any external users of the school systems e.g. adult or community education groups; breakfast or afterschool club

- Take responsibility for liaising with the school on appropriate use of the school's ICT equipment and internet
- Ensure that participants follow agreed Acceptable Use Procedures

Acceptable Use Policies

School have a number of AUP for different groups of users.
These are shared with all users yearly and staff and pupils will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to school who use our IT facilities are made aware of the appropriate AUP.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We will deliver a planned and progressive scheme of work to teach Online Safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity.

We believe that learning about Online Safety should be embedded across the curriculum and also taught in specific lessons in ICT and PSCHE.

We will discuss, remind or raise relevant Online Safety messages with pupils routinely wherever suitable opportunities arise.

We will remind pupils about their responsibilities to which they have agreed through the AUP.

Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter and website.

We will ask all parents to discuss the pupil's AUP with their child and return a signed copy to the school.

We request our parents to support the school in applying the Online Safety policy.

Managing and safeguarding ICT Systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible. Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

Any administrator or master passwords for school ICT systems are kept secure and available to at least two members of staff, e.g. head teacher and member of technical support.

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named individuals e.g. a member of technical support.

We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

Filtering Internet access

Web filtering of internet content is provided by Lancashire LA using 'Netsweeper Filtering'. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. Notices are posted in classrooms and around school as a reminder.

Access

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users.

Detailed guidance on the protection of sensitive school data and information assets is included in the **Lancashire Information Security Guidance** which forms part of this policy.

Using email

Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

E-mails must never be used to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

Use of the school e-mail system is monitored and checked.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

Responsible use of personal web mail accounts by staff is permitted.

n.b. Additional guidance for staff is included in the **Lancashire Electronic Communications Guidance for Staff** and this is included as part of the school's Online Safety Policy.

Publishing content online
e.g. using the School website, Learning Platform, blogs, wikis, podcasts, social network sites
School website:

The school maintains editorial responsibility for any school initiated web site or learning platform content to ensure that content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.
The point of contact on the web site is the school address, e-mail and telephone number. Published contact details for staff are school provided.
Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web site and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Creating online content as part of the curriculum:
As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Blogging, podcasting and other publishing of online content by pupils will take place within the school learning platform or other media selected by the school. Pupils will only be allowed to post or create content on sites where members of the public have access, when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.
We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the school :
Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.
Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.
n.b. Additional guidance for staff is included in the **Lancashire Electronic Communications Guidance for Staff** and this is included as part of the school's Online Safety Policy.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online. We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

n.b Additional guidance for staff is included in the **Lancashire Electronic Communications Guidance for Staff** and this is included as part of the school's Online Safety Policy.

Using video conferencing and other online meetings

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. We ensure that staff and pupils take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Pupils do not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

For their own protection a video conference or other online meeting between a member of staff and pupil(s) which takes place outside school or whilst the member of staff is alone is always conducted with the prior knowledge of the head teacher or line manager and respective parents and carers.

n.b. Additional guidance for staff is included in the **Lancashire Electronic Communications Guidance for Staff** and this is included as part of the school's Online Safety Policy.

Using mobile phones and other mobile devices

We recognise that the multimedia and communication facilities provided by a mobile phone can provide beneficial opportunities for pupils. However their use in lesson time will only be with permission from the teacher.

School mobile phones or similar devices with communication facilities used for curriculum activities are set up appropriately for the activity. Pupils are taught to use them responsibly.

Where required for safety reason in off-site activities, a school mobile phone is provided for contact with pupils, parents or the school. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Unauthorised publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter.

n.b. Additional guidance for staff is included in the **Lancashire Electronic Communications Guidance for Staff** and this is included as part of the school's Online Safety Policy.

Using other technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an Online Safety point of view.

We will regularly review the Online Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

Protecting school data and information

School recognises their obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation as well as all aspects of GDPR – see data policy.

Pupils are taught about the need to protect their own personal data as part of their Online Safety awareness and the risks resulting from giving this away to third parties.

Staff are made fully aware of the contents of the **Lancashire Information Security Guidance for Staff** which is included as part of this policy.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following :

- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- E-mails must never be used to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.
- We have full back up and recovery procedures in place for school data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example Governors or the SIP, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies.

Dealing with Online Safety incidents

All Online Safety incidents are recorded in the School Online Safety Log which is regularly reviewed.
Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.
In situations where a member of staff is made aware of a serious Online Safety incident, concerning pupils or staff, they will inform the Online Safety coordinator, their line manager or head teacher who will then respond in the most appropriate manner. [See **First Response Guidance to Online Safety Incidents]**
Instances of **cyberbullying** will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.
Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Online Safety coordinator and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.
School reserve the right to monitor equipment of their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Kirklees Safeguarding Procedures and Guidance will be followed.

Section 5.1.6 Child Abuse and Information Communication Technology

Dealing with complaints and breaches of conduct by pupils:

. Any complaints or breaches of conduct will be dealt with promptly
. Responsibility for handling serious incidents will be given to a senior member of staff
. Parents and the pupil will work in partnership with staff to resolve any issues arising
. There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

Sexting

. Sexting is when someone sends or receives a sexually explicit text, image or video. This includes sending 'nude pics', 'rude pics' or 'nude selfies'. Pressuring someone into sending a nude picture can happen in any relationship and to anyone, whatever their age, gender or sexual preference.
. However, once the image is taken and sent, the sender has lost control of the image and these images could end up anywhere. By having in their possession, or distributing, indecent images of a person under 18 on to someone else, young people are not even aware that they could be breaking the law as stated as these are offences under the Sexual Offences Act 2003.
.
. Guidance on how to deal with sexting can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

The following local and national guidance are acknowledged and included as part of our Online Safety policy:

1. Lancashire LCSB Guidance

The Lancashire Safeguarding Children's Board Procedures and Guidance

Lancashire Safeguarding procedures will be followed where an Online Safety issue occurs which gives rise to any concerns related to Child Protection. In particular we acknowledge the specific guidance in:
Section 5.1.6 Child Abuse and Information Communication Technology
This section of the Lancashire Safeguarding procedures covers awareness of, and response to, issues related to child abuse and the Internet. In particular we note and will follow the advice given in the following section:

Section 7. Actions to be taken where an Employee has Concerns about a Colleague This provides guidance on the action to be taken if an employee has either information or reason to suspect that a colleague is accessing indecent images of children.

2. DfE Guidance

Guidance for Safer Working Practices for those working with Children and Young People in Educational Settings DfE May 2019

This guidance provides clear advice on appropriate and safe behaviours for all adults working with children in paid or unpaid capacities, in all settings and in all contexts. We acknowledge the guidance given in the following sections and accept this as part of our policy. (See extract in Appendix)

. **Section 12 Communication with Children (including the use of technology)**
. **Section 24 Photography, video and other images**
. **Section 25 Exposure to inappropriate images**

3. A1: Acceptable Use Agreement (Staff, Volunteers and Governors)

4. A2: Acceptable Use Agreements (Pupils – adapted for phase)

5. St. Joseph's Safeguarding Policy

A1: Acceptable Use Agreement (Staff / Volunteers)

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

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 students / pupils learning and will, in return, expect staff and volunteers to 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. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Website etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school / academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school / academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try (unless I have permission) 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 not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school / academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include: a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

A2: Acceptable Use Agreements (Pupils – adapted for phase)

KS2 Pupil Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to make sure 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 school will monitor how I am using the computers and the internet.
- I will keep my username and password safe and secure – I will not share it, and I will not 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" if I am communicating with someone on-line.
- I will not share personal information about myself or others when on-line. I will not share names, addresses, email addresses, telephone numbers, age, whether I am a boy or girl or information about my school.
- I will not arrange to meet people that I have communicated with on-line unless I am taking an adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I am on-line.

I understand that everyone has equal rights to use technology to help them with their work:

- I understand that the computers and other devices are for teaching and learning and I will not use them for anything else unless I have permission.
- I will check with an adult before I download or upload anything that might take up a lot of space and stop others carrying out their work.
- I will not use the school computers or other devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission from an adult to do so.

I will act as I expect others to act towards me:

- I will respect others people's work and property and will not access, copy, remove or change any other user's files, without their knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use bad language and I will respect other people's opinions.
- I will not take or share images of anyone without their permission.

I understand that the school has to keep the computers and other devices it offers me safe and secure to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may hurt or upset others. I will not try to use any programmes or software to bypass the filtering / security systems in place.
- I will immediately report any damage or problems with equipment or software, however this may have happened.
- 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, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to install or store programmes of any type on any school device, or try to alter computer settings.

When using the internet for my work or enjoyment, I understand that:

- I must have permission before I use someone else's work 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 find is correct. I understand that other people may sometimes give information which is untrue or trying to mislead me.

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

- I understand that the school also has the right to take action against me if I do anything when I am out of school involving other members of the school community which breaks the rules in this agreement (e.g. cyber-bullying, using or sharing images or personal information).
- I understand that if I do not follow this Acceptable Use Policy Agreement, I may not be allowed to use the school computers / internet and school will contact my parents. If I use the computers for something which is illegal, school will contact the police.

Please ask a parent/carer to help you to fill in the form on the next page to show that you have read, understood and agree to the rules in the Acceptable Use Agreement.

KS2 Student / Pupil Acceptable Use Agreement Form

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 Agreement. I agree to follow these rules when:

- I use the school computers, website and devices (both in and out of school)
- I use my own equipment out of school as a member of this school (eg communicating with other members of the school, accessing the school website etc.)

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Parent / Carer Countersignature

I too have read and understood the above and agree to help my child follow the guidelines when:

- using the school systems, website and devices (both in and out of school)
- using their own equipment out of the school in a way that is related to them being a member of this school eg communicating with other members of the school, accessing school website etc.

Parent/ Carer Name: .....

Signed: .....

EYFS & KS1 Pupil Acceptable Use Policy Agreement

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
- I know that if I break the rules I might not be allowed to use a computer / tablet

Child's Name: .....

Signed (child): .....

I too have read and understood the above and agree to help my child follow the guidelines.

Parent/ Carer Name: .....

Signed (Parent: .....

Responding to incidents of misuse – flow chart

