



Tibberton CE First School and Hindlip CE First School

Online Safety Policy

Developed using the Worcestershire Schools policy template



The Executive Headteacher Mr A. Gromski

Chair of Governors – Mr A. Clarke

Computing Governor – Mrs L. Pritchard

Date of Adoption by the Governing Body – Spring 25

Date of Review – Annual

Online-safety Co-ordinators- A Gromski / D Burton

'Whatever you do, work at it with all your heart.' Colossians 3:23

This policy will help us maintain a happy, respectful atmosphere and a safe environment for everybody in our schools; it will help us promote fairness and equality at all times and reflects the strong Christian ethos of our schools. As Church of England Schools, we are committed to enabling every person to flourish and live out 'life in all its fullness'. We want our children to grow in wisdom; to cultivate a wide-ranging knowledge that will help broaden life chances; to develop the spiritual, intellectual and emotional resources they need to live a good life; and to develop the character to live well together in community, whilst preparing them for the opportunities, responsibilities and experiences of future life.

This Online-safety Policy should be viewed alongside other relevant policies, including but not limited to; Safeguarding, Behaviour and Anti-Bullying, Anti Radicalisation as well as Use of Images and our Online-Safety Home School Agreement.

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Searching, screening and confiscation](#)
- [Relationships and sex education](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

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

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems & the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the IT leads to make sure the appropriate systems and processes are in place
- Working with the IT lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The IT lead

The IT Lead is responsible, with the support of the Executive Headteacher for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

- What are the issues? – [UK Safer Internet Centre](#)
- Online safety topics for parents/carers – [Childnet](#)
- Parent resource sheet – [Childnet](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

In **Key Stage (KS) 1**, pupils will be taught to:

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

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE)

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

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

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

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search with the support of a colleague and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from SLT
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not view the image**
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)

- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Our School Federation recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Our School Federation will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may NOT bring mobile devices into school

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of [three random words](#), in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, governors and volunteers

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

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

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Appendix 1a – Acceptable Use Agreement – pupil

Rules for Responsible Computer and Internet Usage

The school makes regular use of the Internet to support learning. We expect all pupils to take responsibility for their own behaviour within the wider environment of the school and when using the Internet. This includes materials that they choose to access and the language they use.

Online-safety is very important so these rules will help to keep you safe and help us to be fair to others.

- I will let a teacher/adult know if I find any unpleasant pictures or writing.
- I will only use the Internet when I have been given permission and am being monitored by an adult.
- I will not give out my surname, home address, email address or telephone number.
- I will use the school computers only for schoolwork and homework.
- I will not display offensive messages or pictures.
- Any messages I send will be polite and responsible.
- I will not send an E-mail to anyone until my teacher has approved it.
- I will not download any program files to the computer from the Internet to prevent corruption of data and avoid viruses.
- I will not upload school photographs onto the internet.
- I will not use social media sites at school.

Pupils choosing not to comply with these expectations will receive a warning and subsequently may be denied access to the Internet within school.

I have read this agreement with my parent/guardian and agree to these safety restrictions:

Signed: _____ (Child)

_____ (Parent/Guardian)

Date: _____

Appendix 1b - Acceptable Use Agreement – staff & volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school/academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT 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 ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of the school.
- I understand that the school ICT 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 in the online-safety policy.
- 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 will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

I will be professional in my communications and actions when using school 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 images. I will not use my personal equipment to record these images.
- Where images are published (e.g. on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the online-safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies. (see section A.3.2 of the online-safety policy)
- I will only communicate with pupils and parents / carers using official school/academy systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the online-safety policy)
- 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:

- I will only use my personal mobile ICT devices as agreed in the online-safety policy (see section A.3.1) and then with the same care 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 use personal email addresses on the school ICT systems except in an emergency (A.3.2).
- I will not open any attachments to emails, unless the source is known and trusted, 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/academy policies (Maintained and subscribing establishments see **IBS Schools Systems and Data Security advice**).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or radical material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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.

- 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (see e-security policy). **I understand that where personal data is transferred outside the secure school/academy network, it must be encrypted.**
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- I understand that data protection policy requires that any staff or 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/academy 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 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 school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in the school, but also applies to my use of school/academy ICT systems and equipment out of the school and to my use of personal equipment in the school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and/or the Local Authority and/or other relevant bodies including, in the event of illegal activities, the involvement of the police (see section A.2.6).

I have read and understand the above and agree to use the school/academy ICT systems (both in and out of the school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

Appendix 2: online safety training needs – self-audit for staff

Adapt this form to suit your needs.

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 3: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 4: Guidance to support the safe and appropriate use of images in schools and settings

Based on:

Safeguarding Children and Safer Recruitment in Education – *Consultation version 2010*

Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings – *DCSF March 2009*

Data Protection Good Practice Note: Taking Photographs in School – *Information Commissioner's Office 26th October 2007*

Please ensure that all staff are given copies of this guidance and made aware of school policy

Introduction

There are many occasions when staff and parents will want to take photographs of children. Such occasions include everything from observation, evidence, assessment and curricular purposes in the classroom to award ceremonies, performances, trips and sporting events as part of the extended activities programme. The intention of this policy is to set out clear guidelines which will balance the use of photography as a source of pleasure and pride with the need to safeguard children and protect the rights of the individual.

The photography policy sets out to ensure that:

- Photographs are only used for the purpose intended
- Settings use of photographs is facilitated
- Personal family photography is allowed where possible
- Individual rights are respected and child protection issues considered
- Parents/carers and children are given the right to opt out.

Definitions

The term 'images' refers to photographic prints or slides, digital images, videos or moving images. Images may be distributed via print, DVDs, the internet or other technologies.

The term 'settings' refers to Early Years Settings, Maintained Schools, Independent Schools, Free Schools, Academies, Short Stay Schools, Colleges of Further Education, out of school provision, childminders and Children's Centres.

Safeguarding Children

The welfare and protection of our children is paramount and consideration should always be given to whether the use of photography will place our children at risk. Images may be used to harm children, for example as a preliminary to 'grooming' or by displaying them inappropriately on the internet, particularly social networking sites.

For this reason consent is always sought when photographing children and additional consideration given to photographing vulnerable children, particularly Looked After Children or those in domestic abuse situations. Consent must be sought from those with parental responsibility (this may include the Local Authority in the case of Looked After Children).

Data Protection

The Information Commissioner's Office (ICO) maintains a public register which includes the name and address of 'data controllers' and details about the types of personal information they process. 'Notification' is the process by which each data controller's details are added to the register. All settings need to ensure they are registered with the Information Commissioner's Office every year. Failure to notify the ICO is a criminal offence. Notification is necessary if settings are processing personal information. This includes taking photographs of the children using a digital camera. Personal data (including photos) held by settings must be included in the setting's notification. Further information on data protection as well as details on how to notify can be found at: http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx

In October 2007, the Information Commissioner's Office issued the following advice:

"The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- *Photos taken for official school use may be covered by the act and pupils and students should be advised why they are being taken.*
- *Photos taken purely for personal use are exempt from the Act."*

Please note that although notification is mandatory in most cases the data protection guidance within this document is 'recommended guidance' and settings must take individual responsibility for their own data protection issues in accordance with the Data Protection Act 1998.

Parental Consent

On admission of a child to a setting, parents/carers will be asked to complete a consent form indicating their agreement or objection regarding the use of images of their child. Consent should be discussed with the child, once they are old enough to understand, and the child also asked to sign the consent form. Parents/children should be asked to complete the separate WCC consent form for images that have been taken for the purpose of LA publicity.

A list of children for whom consent has been refused will be maintained by the setting and every effort will be made by staff not to include these children in photographs or video footage. The list will be updated on a regular basis¹.

The parent/carer should be asked to confirm, in writing, that they will inform the setting if they no longer wish images of their child to be used for any reason. They need to be made aware that once images are in circulation or have been published, it may be impossible to remove them, although every effort will be made to ensure they are not used in future publications.

¹ The LA recommends on admission to a setting with at least annual updates

Setting Photography

Photographic and/or video images taken by staff may be used for curricular and/or extra-curricular activities, displays, on the setting website, in the setting prospectus or newsletter, as evidence of the child's development or as part of publicity in the media. Staff will ensure that:

- They are clear about the purpose of the activity and what will happen to the images when the activity is concluded.
- They always use setting equipment for taking images.
- They never record images using their personal camera, mobile phone or video equipment or for their own personal use.
- They will never photograph children in a state of undress, for example whilst changing for PE or a performance.
- They will report any concerns about inappropriate or intrusive photographs found to the Senior Designated Person following the setting's safeguarding procedures
- They have parental permission to take; store and/or display the images.
- Childminding settings should pay particular attention to the safe storage of digital imagery if using their personal equipment to record and store images

Storage of Images

Photographs retained in a setting will not be used other than for their original purpose, unless permission is obtained from the subject.

Images should always be stored securely and password protected.

Photographs should be destroyed or deleted from databases once they are no longer required for the purpose for which they were taken. Photographs taken for publicity and promotional purposes should be retained for a maximum of two years. Photographs contributing to the history of the setting, its children, activities or the community, may be retained indefinitely.

For schools, further information on storage and security can be found in the LA guidance *Schools System and Data Security*.

Parental Photography

In many cases, photographs taken at setting events form an important part of family albums. Everything possible will be done to ensure that this tradition continues. Parents are welcome to take photographs of their own children at award ceremonies, setting concerts/shows and sporting events, with the permission of the Headteacher/Senior Manager or Childminder. However, care must be taken not to interfere with the smooth running of the event, breach commercial copyright laws or compromise health and safety. Parents/carers will ensure that:

- They will respect the setting's decision to prohibit photography of certain children or a particular event.
- Any images taken are for personal use only.
- Images including children **other than their own, must not be sold or put on the internet**; if they are, Data Protection legislation may be contravened and they will be asked to remove them.
- They will not use any images of children so as to cause offence or harm.

The Use of Cameras and Video Recordings by Children

From time to time, children may be given the opportunity to use setting equipment to take photographs and/or video footage as part of a curricular or extra-curricular activity.

Children should not use personal equipment in the setting for the purpose of taking photographs or video footage, unless being used as a learning resource in line with the setting's Acceptable Use policy. This includes the use of personal Smartphones. The only exception to this is on a setting trip or visit where children may be allowed to take photographs for their own personal use.

It should be made clear that these images should be taken responsibly and not used to upset any other child

The use of images to bully or intimidate, including publishing photographs without permission on the internet, will be dealt with in line with the setting's behaviour and anti-bullying policies and may be viewed as a criminal offence.

Display of photographs

It is perfectly acceptable to display photographs of children in the setting environment with their names attached for the purpose of celebrating progress and achievement or assessment purposes.

However, all settings must give consideration to displays when rooms are available for other purposes.

Publicity

Press

On occasions, the media are asked to cover setting events or to highlight children's successes. This is an important part of celebrating achievement and informing the public of educational initiatives. The media operate under their own Code of Practice. Parents will be informed by the setting in advance if their children are likely to appear in the press. Local newspaper titles may share their images with other titles within the same syndicate. Any child whose parents have withheld permission, will not be photographed by the media.

Setting Publicity

Photographs of children's activities and achievements may be published in the setting newsletter or prospectus and posted on the setting website. Names of individual children will not be attached to photographs and no contact details will be published. Where photographic permission has been withheld, photographs will not be published.

Setting Photographer

Class and individual or group photographs are often an annual event. Parents will be notified in advance of the photographer's visit and will be sent copies of photographs and given the option to purchase them. Copyright on all such photographs is retained by the photographer.

Links

This guidance should link specifically to the setting's Data Security Policy, Online-safety Policy, Acceptable Use Policy, Password Policy, Staff Laptop Policy, Safeguarding Children Policy and to the LA guidance 'Schools System and Data Security'.

Further Guidance

Further related guidance can be found in the Becta series of documents entitled *Good practice in information handling in schools*. They are:

- 1 Keeping data secure, safe and legal
- 2 Impact levels and labelling
- 3 Audit logging and incident handling
- 4 Data encryption
- 5 Secure remote access

and also in *AUPs in context: Establishing safe and responsible online behaviours*

These documents can be found on Edulink (www.edulink.networcs.net) and on the Department for Education website (www.education.gov.uk).

Appendix 5 Social Networking Teacher Agreement

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'. In exceptional circumstances this may be modified with the expressed permission of the Head Teacher and the Governors.
- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.
- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.
- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.
- Do not accept pupils (even those that have recently left the school), as 'friends'. You are advised not to have parents or carers of pupils as social media 'friends'.
- Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.
- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.
- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause friction in your school and make your working environment uncomfortable.
- Do not post or upload photographs related to school-based or extra-curricular activities without the expressed permission of the Head Teacher and the Governors. Do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.
- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.
- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.
- ***I understand that injudicious use of social networking may lead to disciplinary action.***
- ***I agree to take all possible precautions as outlined above.***
 - ***I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.***

Name		Date	
Signature			

Appendix 6 Loaned Device User Agreement

Staff member:

Date:

Device Make:

Model :

Serial Number :

The laptop/device detailed above is loaned to _____ for the duration of their employment at Tibberton/Hindlip School subject to the following terms and the school Acceptable Use Agreement.

The iPad/mobile device remains the property of the School and must be returned at the end of the contracted period of employment with the School and, if required, during a planned or prolonged absence.

1. The laptop/device is for the **work related** use of the named member of staff to which it is issued.
2. Only software/apps installed at the time of issue or software/apps purchased by and licensed to Tibberton/Hindlip School may be installed on the machine.
3. The laptop/device remains the property of the School throughout the loan period, however the member of staff to which it is issued **will** be required to take responsibility for its care and safe keeping.
4. If left unattended the laptop/device must be securely stored.
5. Due regard must be given to the security of the computer if using other forms of transport.
6. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality, under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff. Staff should also be cautious when using the computer away from school particularly with files which may contain personal student data, including images.
7. Any networked equipment must be docked in the school charging and syncing cabinet at least once per week to ensure updates and new software are distributed. Staff should record this action in the log provided with the syncing cabinet.
8. The laptop/device will be recalled from time to time for routine maintenance / upgrade and monitoring.

Prohibited Uses

Images of other people, including children, may only be made with the permission of the person, or parents of the child, in the photograph.

The laptop/device is a professional tool designed to enhance classroom practice. It is not for personal use, e.g. Facebook or other social networking sites and should remain in school unless permission is sought from the ICT Co-ordinator or Head Teacher.

Lost, Damaged or Stolen laptop/device

If the laptop/device is lost, stolen or damaged, the ICT Co-ordinator or Head Teacher must be informed immediately and a charge may be levied depending on the circumstances.

I have read and agree to the terms and conditions in this agreement.

I undertake to take due care of the laptop or device and return it immediately upon request.

Signed: _____

Date: _____