St. John's Catholic Primary School
Burscough

# Online Safety Policy

## 2026-2027

Reviewed by Claire Smith

Date September 2026

Date for review: September 2027

**Contents**


| | |
|---|---|
| 1. Introduction | **3** |
| 2. Our school's vision for Online Safety | **3** |
| 3. The role of the school's Online Safety Champion | **4** |
| 4. A co-ordinated approach across relevant safeguarding areas. Policies and practices | **5** |
| 4.1 Security and data management | **5** |
| 4.2 Use of mobile devices including iPads, Pen drives, mobile phones , Blackberries, PSPs, Digital Cameras, Voice recording devices, | **5** |
| 4.3 Use of digital media | **6** |
| 4.4 Communication technologies | **6 - 9** |
| 4.5 Acceptable Use Policy (AUP | **9** |
| 4.6 Dealing with incidents | **10** |
| 5. Infrastructure and technology | **11** |
| 6. Education and Training<br>Online Safety across the curriculum<br>Online Safety – Raising staff awareness<br>All staff made aware of this policy through staff handbook<br>Online Safety – Raising parents/carers awareness<br>Online Safety – Raising Governors' awareness | **11 - 12** |
| 7. Standards and inspection | **12** |
| 8. Appendices | **13-19** |

## 1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact. This policy will also work alongside the GDPR rationale.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in four main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

## 2. Our school's vision for Online Safety

Our school provides a diverse, balanced and relevant approach to the use of technologies, especially as the children move further up the school. Children are encouraged to maximise the benefits and opportunities that technology has to offer including various recording technologies, iPads, use of cloud storage on Apple devices, and continued use of desktop computers. As a whole staff, we ensure that children learn in an environment where security measures balance appropriately with the need to learn effectively. All the children throughout school are aware of the SMART rules. Following these rules ensures that children are equipped with the skills and knowledge to use technology appropriately and responsibly; thus becoming a good digital citizen.

As a school, we will teach our children to recognise the risks associated with technology and how to deal with them, both within and outside the school environment, in IT, SMSC, British Values and PSHE lessons. The focus should be on managing risk not blocking it out altogether; giving the children strategies for use in later life and being positive in their behaviours online.

All users in our school community understand why there is a need for an Online Safety Policy.

## 3. The role of the school's Online Safety Champion

**Our Online Safety Champion is Miss Claire Smith who is Head teacher and DSL**

The Online Safety Champion is the nominated point of contact within the school for Online Safety-related issues and incidents. However, certain responsibilities may need to be delegated to other staff e.g. Subject leader or Designated Senior Person/Child Protection Officer as is necessary.

The role of the Online Safety Champion should include:

Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including:

- Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring any Online Safety Incident is logged and reported to the Head teacher.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools ICT Team and website and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP). This will be updated on the school website and reported to parents where relevant on an e-safety tab.
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the Head teacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer (SK) keeping records of any 'suspicious searches' in the subject leader file.

## 4. A co-ordinated approach across relevant safeguarding areas.

## Policies and practices…

### 4.1 Security and data management

In line with the requirements of the General Data Protection Regulation (GDPR) 2018, sensitive or personal data is recorded, processed, transferred and made available for access in school where appropriate and where necessary. All data from year six pupils will be passed on to their high school with a signed receipt of new ownership. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- And importantly, only transferred to others with adequate protection.

*In our school, personal and confidential data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:*

### 4.2 Use of mobile devices:

*In our school, we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:*

- That some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content. If Wi-Fi is enabled on the device, this device can be found by others outside of the school community
- Is it encrypted?
- Any devices used outside of school are virus checked before use on school systems
- Children are taught to use apps in a responsible manner appropriate to age and task

## 4.3 Use of digital media

*In our school, we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.*

As photographs and video of pupils and staff are regarded as personal data in terms of GDPR (2018), school must have written permission for their use from the individual and/or their parents or carers. **See Appendix 2.**

An opt-in form must be sent to parents from Reception to ensure we have permission from them to use their child's image and ensure that consent is given by staff or parents who are likely to appear in any photographs/video.

Staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs. Children's first name and surname together will never be used on the website, Facebook or any other digital platform alongside a photograph.

Parents/carers, who have been invited to attend school events (school plays/sports days etc), are allowed to take videos and photographs, but are asked not to publish them online or on personal websites where anyone can view them. (Emphasise private profiles.)

All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites and are asked to keep their pages private and not available for public viewing.

Staff should use only school cameras or Class iPads to take pictures of the children and when taking photographs/video and will ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.

All staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.

We will ask permission for photographs to be used after the child has left for marketing publicity.

## 4.4 Communication technologies

*In our school, the following statements reflect our practice in the use of email.*

It is recommended that all users have access to the Lancashire Grid for Learning service as the preferred school e-mail system. Our school bursar is able to set up new accounts for both staff and pupils.

Only official email addresses should be the only one used to contact parents/pupils. The office 365 e-mails provided by county are also encrypted user to user.

The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of repeated SPAM should be reported to the subject leader.

All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.

All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.

All users, both staff and/or pupils, must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

*In our school, the following statements outline what we consider acceptable and unacceptable use of Social Network sites:*

The use of social networking sites has over recent years become the primary form of communication between friends and family. In addition, many other sites allow people to publish their own pictures, text and video. Social Network sites allow users to be part of a virtual community. Current popular examples of these are Face book, You Tube, Instagram, Twitter, Minecraft and Club Penguin. Sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments. It is widely acknowledged that use of such sites does not provide a completely private platform. Even when utilised sensibly and with caution employees cannot control comments or images published by others, which may portray the employee in a manner that is not appropriate to their role in school. Within school, children will only ever publish work on SeeSaw and our school website.

All staff need to be aware of the following points – These will be highlighted in our first staff meeting of the year:

- They should not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites. No online 'friendships' are made whilst employed by school as this could lead to professional relationships being compromised.
- No staff will access their private social media account whilst at school.
- Any adult employed by St John's Catholic Primary School must not communicate with pupils using any digital technology where the content of the communication may be considered inappropriate or could be misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Dating sites will never be accessed in school.
- Staff should not use social networking sites to 'vet' prospective employees. Such practice could potentially create an un-level playing field and lead to claims of discrimination.
- Current pupils should **never** be added as 'friends' on any Social Network site. It is unwise to add past pupils, particularly under the age of 18.
- Children are taught to use blogs appropriately and to speak on there as they would face-to-face with anyone.
- Staff are reminded that when they appear on Zoom they could be recorded by parents or other adults at the other end of a screen and to behave with this in mind.

*Remember; whatever means of communication you use, you should always conduct yourself in a professional manner. If content is made available on the web, it is available for everyone to see and remains there forever.*

**In our school, the following statements outline what we consider acceptable and unacceptable use of Mobile telephones:**

Mobile phones are not permitted in school for children's use. Staff should ensure their own phones are turned off/silent and not used in the classroom. Sending text messages and making phone calls should, wherever possible, be avoided in the staff room as a common courtesy to other staff room users.

It is acceptable to use personal mobile phones for contact during school activities e.g. school trips. However, it **should never** be used for photographs. Teacher iPads will be taken on trips for photographs.

A school mobile phone is made available for activities where a personal mobile phone maybe considered inappropriate, i.e. Out of School club and school kitchen for emergency calls.

Text messages are sent out to parents to give notification of club times and messages. These are only sent via the bursar and where relevant, after the Head teacher's approval.

Should a child ever have a mobile phone in school, it is to be confiscated and locked in the bursar's office and is only available for parents or carers to pick up at the end of the day. Staff should never (unless there is cause for concern) look at images on a child's phone.

*In our school, the following statements outline what we consider acceptable and unacceptable use of Instant Messaging:*

This popular tool used by adults and pupils allows 'real time' communication and often integrates the ability to transmit images via a webcam. Although these sites are 'blocked' for use in Lancashire schools by default, some exceptions are made, see video conferencing. Snap chat and other similar sites should never be used in school.

Staff and children are aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts.

*In our school, the following statements outline what we consider acceptable and unacceptable use of websites and other online publications:*

Lots of work and constant updates occur on our school website. As a staff, we will ensure that our school website is effective in communicating Online Safety messages to parents/carers. (SMART rule updates on each class page.)

Everyone in the school is made aware of the guidance for the use of digital media on the website, Staff will update their own class pages with their own log on addresses – this will mean we can monitor who and what is posted online as a representation of our school. Any member of the Teaching staff can post content onto our Facebook page.

It is made clear there are to be no pictures linked to full names.

Content is always considered subject to copyright/personal intellectual copyright restrictions and all information on our school website is available for everybody to see.

Any downloadable materials are in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without our school's consent (except on the private Governors section where edits are required)

*In our school, the following statements outline what we consider acceptable and unacceptable use of live streaming:*

The relevant permissions letter is made available for parents/carers to sign giving permission for their child/children to participate in video and photographs. Children should never be appearing 'live' on the Internet through a video conferencing link without two members of staff present at all times. It is still important to remember that the images, which are broadcast from school, could be captured as a snapshot or video clip from a system receiving the broadcast. Face time calls should never be used on staff mobile phones on the school premises.

Approval by the Head teacher must be obtained in advance of live lessons via Zoom. This would happen as a result of a school closure.

Children are taught to behave appropriately, to have their cameras on to show that it is them online and not someone else, to take turns in speaking and behave impeccably in front of other peers. Children use the live chat facility whilst live and online and this too is a skill to teach acceptable and appropriate usage of.

## Others:

*As we risk assess and introduce new technologies we will need to update our policy to reflect what we consider acceptable and unacceptable use of these.*

## 4.5 Acceptable Use Policy (AUP)

*As attached in Appendix and signed copies to be kept with the Head teacher.*

## 4.6 Dealing with incidents

### Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Online Safety leader who will then log and pass on to Head teacher who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF).

**We will never personally investigate, interfere with or share evidence as we may inadvertently be committing an illegal offence.** It is essential that correct procedures be followed when preserving evidence to protect those investigating the incident (http://www.iwf.org.uk). These groups are licensed to investigate – schools are not.

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Some examples of inappropriate incidents are listed below with suggested sanctions.

## Incident Procedure and Sanctions

- Accidental access to inappropriate materials.
    - Minimise the webpage/turn the monitor off then tell a trusted adult.
    - Enter the details on CPoms and report to LCC filtering services, if necessary.
    - Persistent 'accidental offenders' may need further disciplinary action.
- Using other people's logins and passwords maliciously.
    - Inform SLT or designated Online Safety Champion.
    - Enter on CPOMS
    - Raising awareness of Online Safety issues and the AUP with individual child/class.
    - More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
    - Consider parent/carer involvement.
- Deliberate searching for inappropriate materials.
    - Inform SLT or designated Online Safety Champion.
    - Enter the details on CPOMS
    - Raising awareness of Online Safety issues and the AUP with individual child/class.
    - More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
    - Consider parent/carer involvement.
- Bringing inappropriate electronic files from home.
    - Consider parent/carer involvement.

## 5. Infrastructure and technology

*As a school, we are responsible for ensuring that your infrastructure /network is as safe and secure as possible.*

**Access:**

Pupils can only log onto a computer with their year group domain username. We currently have 30 desktops in school and 54 iPads.

The administrator password – is kept private from all staff

Staff have individual logins with their own password and transferrable desktops. They also have access to the 'Teacher Share' section of the network. This is not accessible by pupils and guest logins.

There is a separate network for the Head teacher and bursar.

**Passwords:**

All the staff logins are password protected.

**Software/hardware:**

Our IT technician regularly updates computers and checks hardware.

**Managing the network and technical support:**

The school buys in the support of an IT technician from LCC for half a day every month. School bursar Ruth Harrison-Scott is available to provide in house support daily.

**Filtering and virus protection:**

All our computers are Sophos protected and are monitored through LCC. We now have devolved filtering using the BT Light Speed system, and staff can ask for websites to be 'unblocked' via the Light speed system. You Tube is open when staff log-in with a staff log-in. It is blocked when children log-in.

## 6. Education and Training

Education and training are essential components of effective Online Safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online Safety guidance must be embedded within the curriculum and advantage taken of new opportunities to promote Online Safety. This can be done through discreet IT lessons, or PSHE using National Online Safety Resources*. Staff should never say the internet is not safe – it is about managing age appropriate risk.*

## 6.1 Online Safety across the curriculum

All staff are expected to promote and model responsible use of IT and digital resources. Regular updates on Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed in staff and SLT meetings.

## 6.2 Online Safety – Raising staff awareness

All staff are made aware of this policy through our staff handbook and annually at the first staff meeting of each school year. Updates are added to relevant staff meetings. Monthly online safety letters are now published on our website and on Facebook page for both staff and parents to access and signpost them to appropriate resources.

## 6.3 Online Safety – Raising parent's/carers awareness

"*Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it*." (Byron Report, 2008).

Our school offers regular opportunities for parents/carers and the wider community to be informed about Online Safety, including the benefits and risks of using various technologies through notes for parents on the 'Safeguarding tab' of the website and guidance from CEOP.

Parents can access a wealth of online safety information on our website with our monthly newsletters – all of which are labelled with their main focus – eg. fortnite chatting, TikTok, Snapchat, Facebook etc

## Safety – Raising Governors' awareness

Governors are to be made aware of this policy and any updates via termly governor meetings. An Online Safety link governor is named and works alongside our safeguarding governor. Governors are also reminded that they can access the parent's online safety section of the website to read our newsletters.

## 7 Standards and inspection

As a school, we should consider on a regular basis:

- How will we know if our Online Safety policy is having the desired effect?
- How are Online Safety incidents monitored, recorded and reviewed?
- Who is responsible for monitoring, recording and reviewing incidents?
- Is the introduction of new technologies risk assessed?
- Are these assessments included in the Online Safety Policy?
- Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children? How can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents?
- How does the monitoring and reporting of Online Safety incidents contribute to changes in policy and practice?
- How are staff, parents/carers, pupils and governors informed of changes to policy and practice?
- How often are the AUPs reviewed and do they include reference to current trends and new technologies?
- Does this policy work alongside our GDPR code of conduct?

**APPENDIX 1 – Image and Work Consent Form**

**Name of the child's parent/carer: _____**

**Name of child: _____**

**Year group**: _____

We regularly take photographs/videos of children at our school. These may be used, in our school prospectus, in other printed publications, on our school website, Facebook, blog, or in school displays.

Occasionally, our school may be visited by the media who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes. Children's full names will never appear with their picture. Pictures of children in swimsuits or similar clothes will never be taken.

**In order that we can protect your child's interests, and to comply with the General Data Protection Regulation (2018) please read the Conditions of Use on the bottom of this form. We would ask that you please tick each box, sign, date and return the completed form (one for each child) to school as soon as possible.**

1. I DO agree to my child's photograph being used in printed school publications and for display purposes even after they may have left school.

2. I DO agree to my child's image being on the school website and Twitter account

3. I DO give permission for school to film my child

4. I WILL allow my child to appear in the media as part of school's involvement in an event

5. I DO give permission for my child's work and photograph to appear on the school Facebook page

**I have read and understand the conditions of use attached to this form**

Parent/Carer signature: _____

Name (PRINT): _____

Date: _____

**Conditions of Use**

1. This form is valid for this academic year September 2024-August 2025

2. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website/blog or in any of our printed publications.

4. If we use photographs of individual pupils, we will not use the full name of that pupil in any accompanying text or caption.

5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.

6. We will only use images of pupils who are suitably dressed and not seen to be in a compromising position.

7. Parents should note that websites could be viewed throughout the world and not just in the United Kingdom, where UK law applies.

## APPENDIX 2 - ICT Acceptable Use Policy (AUP) – Staff and Governor Agreement

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

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will be an active participant in Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.

5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

6. I will respect copyright and intellectual property rights.

7. I will ensure that all electronic communications with pupils and other adults are appropriate.

8. I will not use the school system(s) for personal use during working hours.

9. I will not install any hardware or software without the prior permission of Shaun Kearon or ICT SL.

10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.

11. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

12. I will report any known misuses of technology, including the unacceptable behaviours of others.

13. I have a duty to respect the technical safeguards that are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

14. I have a duty to report failings in technical safeguards that may become apparent when using the systems and services.

15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other user's data, or compromise the privacy of others in any way, using any technology, is unacceptable.

16. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

18. I will help pupils to be safe and responsible in their use of IT and related technologies.

19. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

**User Signature**

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

Signature …… Date ……

Full name and role…… (PRINT)

# KS2 Acceptable Use Policy

Staying safe whilst using the computer

## To help me stay safe on the computer...

I will ask permission before using the Internet and use it for a specific purpose.

I will never share my personal details, such as my full name or address, with people I don't know.

I will never share my password with anyone.

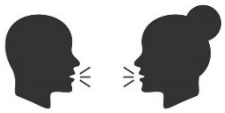
I will never meet up with someone I have met on the Internet.

I will always check my messages are polite before I send them.

I will not reply to a message that isn't kind, but I will save it and show it to an adult.

I will not open or download a file unless I am sure it is safe.

I know I should not believe everything I read on the Internet.



I will always tell an adult if something on the Internet makes me or my friends unhappy.

# KS1 Acceptable Use Policy

Staying safe whilst using the computer

## To help me stay safe on the computer...

I will only use a computer when an adult tells me I can.

I will keep my password safe and not share it with anyone

I will always send polite messages

I will tell an adult if I see something on the computer that makes me unhappy

# EYFS Acceptable Use Policy

Staying safe whilst using the computer

I will only use a computer when an adult tells me I can.

I will tell an adult if I see something on the computer that makes me unhappy

## Staff Acceptable Use Policy

*Staying safe whilst using the computer*

I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.

**Accessing computer systems**

- I will not reveal my password(s) to anyone and will not record it in place where it could be easily discovered (such as the back page of a diary).
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.

**Data Protection**

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and will do everything I can to protect the data from being accessed by unauthorised people.
- I understand that the Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

**Keeping children safe**

- I will embed the school's e-safety curriculum into my teaching and teach children in my care about the e-safety and anti cyberbullying rules.
- I will be vigilant about e-safety risks and incidents (including cyber-bullying) that children in my charge might experience and respond promptly by following the agreed procedures and communicating concerns to the ICT co-ordinator or nominated child protection officer as appropriate.

**Digital Images**

- If I use personal digital cameras or camera phones for taking and transferring images of pupils or staff for professional purposes, I will save the photos on the school network and delete them from my equipment at the first available opportunity.
- I will not store images or photos of children or staff at home without permission.
- I will ensure that I do not photograph or video children for which release permission has not been granted. I will follow the school's guidance document on publication of photographs and videos.

**Communications**

- I will only use the approved, secure e-mail system(s) for any school business. (This is currently the LGfL provided StaffMail system.)
- I will only use the approved school e-mail, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

**Inappropriate Material**

- I will not browse, download or send material that could be considered offensive. This could include (but does not exclusively include) materials that are pornographic, hateful, racist, sexist, abusive, obscene or discriminatory.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the School Bursar.
- I understand that all Internet and network usage can be logged and this information could be made available to my manager on request.

**Copyright**

- I will not publish or distribute work that is protected by copyright.

**Protecting the network & antivirus**

- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet if it does not have up-to-date anti-virus software (or been scanned first for USB flash drives), and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

**Personal use of online publishing systems**

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not make contact with children known to me through school on any social networking site.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.