

## Sacred Heart Catholic Primary School Preston

### Online Safety Policy

July 2026

Review: July 2027

#### **Scope of the Policy**

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online behaviour that take place out of school.

#### **Roles and Responsibilities**

The following section outlines the Online roles and responsibilities of individuals and groups within the school.

##### **Governors / Board of Directors:**

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Governor (it is suggested that the role may be combined with that of the Child Protection / Safeguarding Governor). The role of the Online *Governor / Director* will include:

- *regular meetings with the Online Safety Co-ordinator / Officer*
- *regular monitoring of Online incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors / Board / committee / meeting*

##### **Head teacher and Senior Leaders:**

- The Head teacher has a duty of care for ensuring the safety (including Online) of members of the school community, though the day to day responsibility for Online will be delegated to the Online Co-ordinator
- The Head teacher / Senior Leaders are responsible for ensuring that the Online Safety/ Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their Online roles and to train other colleagues, as relevant.

- The Head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online Co-ordinator.

### **Online Coordinator / Officer**

#### **Head teacher working alongside the ICT subject leader:**

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

### **Technical staff:**

Technical Staff / Co-ordinator Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required Online technical requirements and any Local Authority / other relevant body Online Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with Online technical information in order to effectively carry out their Online role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

### **Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Head teacher/Senior Leader /Online Safety Coordinator) for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.

] Online Safety issues are embedded in all aspects of the curriculum and other activities

- students / pupils understand and follow the Online Safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

**DSL:**

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online bullying

**Students / pupils:**

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online bullying.
- should understand the importance of adopting good Online practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school

## **Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online campaigns

/ literature. Parents and carers will be encouraged to support the school promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

## **Policy Statements**

### **Education – pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online risks and build their resilience.

**Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:**

- A planned Online Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet.
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

### **Education – parents / carers**

Many parents and carers have only a limited understanding of Online risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day

### **Education & Training – Staff / Volunteers**

It is essential that all staff receive Online training and understand their responsibilities, as outlined in this policy.

All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.

- The Online Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

### **Technical – infrastructure / equipment, filtering and monitoring**

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical
- There will be regular reviews and audits of the safety and security of school academy technical systems
- All users will have clearly defined access rights to school / academy technical systems and devices.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place – They are held by BlueOrange.
- The school is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored There is a clear process in place to deal with requests for filtering changes.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). - Invero.
- Appropriate security measures are in place (to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
-

- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### **Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images. The Head teacher reserves the right to instruct parents not to take photos and videos if he/she believes there is a risk of them being used inappropriately and in a way which violates school policy.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

The school must ensure that:

It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

It has a Data Protection Policy

It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)

Risk assessments are carried out

It has clear and understood arrangements for the security, storage and transfer of personal data

Data subjects have rights of access and there are clear procedures for this to be obtained

There are clear and understood policies and routines for the deletion and disposal of data

There is a policy for reporting, logging, managing and recovering from information risk incidents

There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

**Staff must ensure that they:**

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

### **Communications**

When using communication technologies, the school considers the following as good practice:

- **The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and students / pupils or parents / carers (email, Class Dojo, etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Pupils should be taught about Online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

## **Social Media - Protecting Professional Identity**

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, online bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

Clear reporting guidance, including responsibilities, procedures and sanctions Risk assessment, including legal risk

School staff should ensure that:

No reference should be made in social media to pupils, parents/carers or school staff

They do not engage in online discussion on personal matters relating to members of the school community

Personal opinions should not be attributed to the school or local authority Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

## **Unsuitable / inappropriate activities**

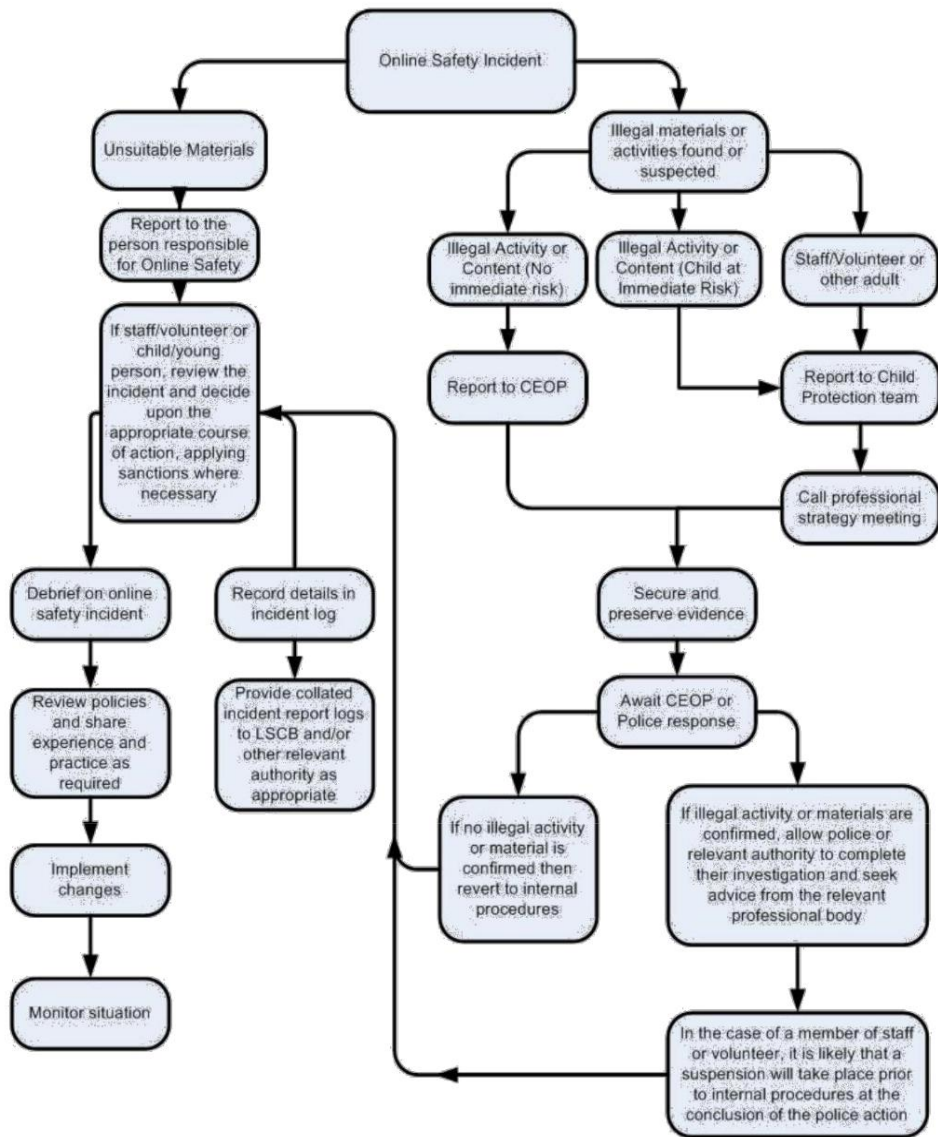
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

### **Responding to incidents of misuse**

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

### **Illegal Incidents**

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



## Other Incidents

**In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise.

- Use the same computer for the duration of the procedure.

It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- a) Internal response or discipline procedures as appropriate.

- b) Involvement by Local Authority or national / local organisation (as relevant).
- c) Police involvement and/or action

**If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

- i. incidents of 'grooming' behaviour
- ii. the sending of obscene materials to a child  
adult material which potentially breaches the Obscene Publications Act
- iii. criminally racist material
- iv. other criminal conduct, activity or materials

**Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

### **School Actions & Sanctions**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedure

## **APPENDIX 1 ICT Acceptable Use Policy (AUP) – Staff and Governors**

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

- ☐ I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- ☐ 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.
- ☐ I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
- ☐ I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat
- ☐ I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.  
I will respect copyright and intellectual property
- ☐ rights.
- ☐ I will ensure that all electronic communications with children and other adults are appropriate.  
I will not use the school system(s) for personal use during working
- ☐ hours.
- ☐ 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.
- ☐ I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
- ☐ I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
- ☐ I will report any known misuses of technology, including the unacceptable behaviours of others.
- ☐ I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
- ☐ I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- ☐ I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to

access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

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

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.

I will take responsibility for reading and upholding the standards laid out in the AUP. I  will support and promote the school's Online Safety policy and  help children to be safe and responsible in their use of ICT and related technologies.

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

**User Signature**

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

Signature

.....

Date .....

Full Name

.....(PRINT)

Position/Role

.....

**APPENDIX 2**

**ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.**

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

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

**User Signature**

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

Signature

.....

Date

.....

Full Name

.....(PRINT)

Position/Role

.....

**Appendix 7**

| <b>Date/Time<br/>Of<br/>incident</b> | <b>Type of<br/>Incident</b> | <b>Name of<br/>pupils/<br/>and staff<br/>involved</b> | <b>System Details</b> | <b>Incident details</b> | <b>Resulting actions taken and<br/>by whom (and signed)</b> |
|--------------------------------------|-----------------------------|---|-----------------------|-------------------------|---|
|                                      |                             |   |                       |                         |   |
|                                      |                             |   |                       |                         |   |
|                                      |                             |   |                       |                         |   |
|                                      |                             |   |                       |                         |   |
|                                      |                             |   |                       |                         |   |
|                                      |                             |   |                       |                         |   |
|                                      |                             |   |                       |                         |   |