# St Joseph's Catholic Primary School, Wallasey

# E-Safety Policy

## Mission Statement:

*"Love one another as I have loved you"*

*John 15:12*

## School Values:

| |
|---|
| *Service* |
| *Justice* |
| *Love* |

## School Vision:

**We seek to build a welcoming, caring community of faith, where we love and serve our children to support them to gain all the necessary spiritual, academic, personal and social skills to succeed in our local and global community.**

**Adopted by Governors: June 2024**

**To be reviewed: June 2026**

Contents

Policies referred to in this document:-

- Behaviour Policy
- Antibullying Policy
- Guest network access policy – we don't have one?
- Electronic Information, Communication and Systems Policy March 2024
- Information Security Policy March 2024
- Data Breach Policy 2021
- Social Media Policy,
- Data Protection Policy 2021
- CCTV Policy Feb 2024
- School Privacy Notice
- School Technical security Policy

## Development / Monitoring / Review of this Policy

This E-Safety policy has been developed in consultation withL
• Headteacher / Senior Leaders
• E-Safety Lead and Subject Leaders
• Staff – including Teachers, Support Staff, Technical Staff
• Governors
• Parents and Carers

### Schedule for Development / Monitoring / Review

| | |
|---|---|
| This E-Safety policy was approved by the Governing Body / Governors<br>Sub Committee on: | |
| The implementation of this E-Safety policy will be monitored by the: | Safeguarding Governor –<br>Headteacher – Mrs Hollis<br>Senior Leadership Team – Mrs Boekweit-Hughes<br>Computer Lead – Mr Clare |
| Monitoring will take place at regular intervals: | Monthly<br>Hi – Impact technician will raise any concerns on the weekly visit |
| The E-Safety Policy will be reviewed annually by staff and Governors, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place. The next review date will be : | March 2025 |
| Should serious E-Safety incidents take place, the following external<br>persons / agencies should be informed: | CADT.<br>CEOP |

### Scope of the Policy

This policy applies to all members of the school (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 Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix). In the case of both acts, action may only be taken over issues covered by the published Behaviour Policy.

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 E-Safety behaviour that take place out of school.

## Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

### Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Standards Committee receiving regular information about E-Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety – Mr B Sharp
. The role of the E-Safety Governor will include:

- regular meetings with the member(s) of SLT responsible for E-Safety
- regular monitoring of E-Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

### Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community; the day to day responsibility for E-Safety will be delegated to all SLT.

The Headteacher and the other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. (See flowchart on dealing with E-Safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Cooks Lawyers HR)

- The Headteacher / Senior Leaders are responsible for ensuring that Year Leaders and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher / 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 E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

### E-Safety Lead:

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

### Hi-Impact Technical staff:

Technical Staff for Computing are 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 E-Safety technical requirements and any statutory guidance that may apply.
• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed where and when appropriate.
• the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
• that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
• that the use of the network / internet / Virtual Learning Environment / Twitter/remote access / email is
regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety Lead for investigation / action / sanction. The approach needs to be evaluated regularly in light of new developments and methods.

### Teaching & Support Staff

are responsible for ensuring that:
• they have an up to date awareness of E-Safety matters and of the current school E-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 Headteacher / Senior Leader ; E-Safety Lead for investigation/ action / sanction.
• all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
• E-Safety issues are embedded in all aspects of the curriculum and other activities
• pupils understand and follow the E-Safety and acceptable use policies
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
• 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.

### Child Protection Officer:

Should be trained in E-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
• cyber-bullying

### Pupils:

• are responsible for using the school digital technology systems in accordance with the 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 cyber-bullying.
• should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
• will experience E-Safety training as part of their curriculum each year.

### 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 / VLE and information about national / Twitter/ local E-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-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 / VLE and on-line / pupil records
• their children's personal devices in the school(where this is allowed)

### Students/Work Experience/Volunteers/Community Users:

Students/Work Experience/Volunteers/Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA (Acceptable Use Agreement) before being provided with access to school systems.

## 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 E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

**E-safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum.The E-Safety curriculum should be broad,**

**relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:**

• A planned E-Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
• Key E-Safety messages should be reinforced as part of a planned programme of assemblies and class council and pastoral activities
• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
• 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 and mobile devices in lessons where internet use is pre-planned, it is best practice that 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and insist in the use of safe search engines.
• It is accepted that from time to time, for good educational reasons, pupils may need to research topics 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 E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line 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, website, Twitter
• Parents / Carers evenings / sessions
• High profile events / campaigns eg E-Safety workshops for parents and children
• Reference to the relevant web sites / publications eg www.saferinternet.org.uk/ http://www.childnet.com/parentsand-carers (see school website and appendix for further links / resources)

## Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's ESafety knowledge and experience. This may be offered through the following:

● Providing family learning courses in use of new digital technologies, digital literacy and E-Safety
● E-Safety messages targeted towards grandparents and other relatives as well as parents.
● The school website will provide E-Safety information for the wider community
● Where and when appropriate supporting community groups eg Early Years Settings, Child-minders, youth / sports /voluntary groups to enhance their E-Safety provision. (www.onlinecompass.org.uk).

## Education & Training – Staff / Volunteers

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process.

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

• The E-Safety Lead will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.

• This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

• The E-Safety Lead 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 previous sections will be effective in carrying out their E-Safety responsibilities:

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

• There will be regular reviews and audits of the safety and security of school technical systems.

• Servers, wireless systems and cabling must be securely located and physical access restricted (stock cupboard/port boxes located around school).

• All users will have clearly defined access rights to school technical systems and devices.

• All users will be provided with an initial username and secure password by Hi Impact who will keep an up to date record of users and their usernames. Staff users are responsible for the security of their username and password and will be required to change their password where and when appropriate.

• The master/administrator passwords are stored on Last Pass which is maintained by Hi Impact.

• The School Business Manager in liaison with the technician 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 is filtered by the broadband/filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored by Hi Impact and Securus monitoring systems.

• 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. (see appendix)

• An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. (Data Breach Policy)

• 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 who by Fortigate by Talk Straight. The school infrastructure and individual workstations are protected by up to date virus software.

• An agreed procedure is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.

• An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school. (Electronic Information, Communication and Systems Policy March 2024/Information Security Policy March 2024)
• An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices. (Electronic Information, Communication and Systems Policy March 2024/Information Security Policy March 2024)
• An agreed policy is in place regarding the use of removable media (eg 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. (see Parent/Pupil Privacy notice in the appendix for further detail). (Electronic Information, Communication and Systems Policy March 2024/Information Security Policy March 2024)

## 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 Cyber 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 and will implement policies to reduce the likelihood of the potential for harm:
• 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 in 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.
• 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 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 pupils are published on the school website (covered as part of the AUA signed by parents or carers at the start of Foundation Stage or when the child joins the school - see Parents / Carers Acceptable Use Agreement in the appendix)
• 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 UK General Data Protection Regulation (UK GDPR) which states that personal data must be:
• Fairly and lawfully processed in a transparent manner
• Processed for specific, explicit and legitimate purposes
• Adequate, relevant and limited to what is necessary
• Accurate and up to date
• Kept no longer than is necessary
• Processed in a manner that ensures appropriate security of the personal data

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". (see Privacy Notice section in the appendix)
● It has a Data Protection Policy (see appendix for policy)
● It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
● 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.
When personal data is stored on any portable computer system, memory stick or any other removable media:
• the data must be encrypted and password protected
• the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
• the device must offer approved virus and malware checking software
• 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 and pupils 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 pupils or parents / carers (email, chat, VLE 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.**
• Whole class / group email addresses may be used at KS1, while pupils at KS2 may be provided with individual school email addresses for educational use.
• Pupils should be taught about E-Safety 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, cyber 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.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and E-Safety committee to ensure compliance with the Social Media, Data Protection, Electronic Information, Communication and Systems Policy March 2024.

## 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 encourage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows :-

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, materials, remarks, proposals or comments that contain or relate to : | Child sexual abuse images – The making, production or distribution of indecent images of children contrary to the Protection of Children Act 1978 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary | | | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| | to the Criminal Justice and Immigration Act 2008 | | | | | |
| | criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986 | | | | X | X |
| | Pornography | | | | X | |
| | promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the | | | | X | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | school into disrepute | | | | | |
| Using school systems to run a private business | | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | | | | | X | |
| Infringing copyright | | | | | X | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the Internet) | | | | | | |
| Online Gaming | | | | | X | |
| Online Gambling | | | | | X | |
| Online shopping/commerce | | | X | | | |
| File sharing | | | | X | | |
| Use of social media | | | X | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Use of messaging apps | | | X | | | |
| Use of video recording, ie You Tube | | | X | | | |

## 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” on previous page).

## 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

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. 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:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- 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.

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 procedures.

# APPENDICES

# Pupil Acceptable Use Agreement for Key Stage 2 Pupils

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

## This Acceptable Use Policy is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other digital
technologies for educational, personal and recreational use.
• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning andwill, in return, expect the pupils to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use school 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.

## For my own personal safety:

• I understand that the school will monitor my use of the systems, devices and digital communications.
• I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
• I will be aware of "stranger danger", when I am communicating on-line.
• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
• If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

• I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal use unless I have permission.

• 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 use the school systems or devices for on-line gaming, file sharing, or video broadcasting (eg You Tube), unless I have permission of a member of staff to do so.

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

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

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

• I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
• I will immediately report any damage or faults involving equipment or software, however this may have happened.
• I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person /organisation who sent the email.
• I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
• I will only use social media sites with permission and at the times that are allowed.

**When using the internet for research or recreation, I recognise that:**
• I should ensure that I have permission to use the original work of others in my own work.
• Where work is protected by copyright, I will not try to download copies (including music and videos).
• When I am using the internet to find information, I should take care to check that the information that access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

**I understand that I am responsible for my actions, both in and out of school:**
• I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, internal exclusion, fixed term exclusion, contact with parents and in the event of illegal activities involvement of the police.

***Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.***

Signed (child):……

Signed (parent): ……..

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

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

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

Signed (parent): ……..

# Parent / Carer
# Acceptable Use Agreement

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

## This Acceptable Use Policy is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
• that parents and carers are aware of the importance of E-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

## Permission Form

Parent / Carers Name

….....

Pupil's name
……

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to IT systems at school.

Either: (KS2 and above)
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, E-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, E-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's E-Safety.

Signed …… Dated……

# St Joseph's Primary School's Foundation Stage and KS1 E-Safety Code

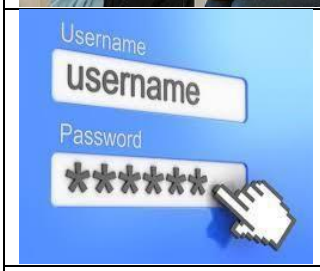
## Think then click …

## These rules help us to stay safe on the internet

| | |
|---|---|
|  | We only use the internet when an adult is with us. |
|  | We can click on the buttons or links when we know what they do. |
|  | We can search the Internet with an adult. |
|  | We always ask if we get lost on the internet |

# St Joseph's Primary School's KS2 E-Safety Code

## Think then click …

| | |
|---|---|
|  | We ask permission before using the internet. |
|  | We only use websites our teacher has chosen. |
|  | We tell an adult if we see anything we are uncomfortable with. |
|  | We never give out personal information or passwords. |
|  | We never arrange to meet anyone we don't know. |

**St Joseph's Primary School**
**STAFF/VOLUNTEER ACCEPTABLE USE POLICY AND AGREEMENT (2021)**

## Introduction

This policy is designed to enable acceptable use for staff and governors.
The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.
This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.
The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.
If you are in doubt and require clarification on any part of this document, please speak to the Business Manager.

## Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.
No personal equipment should be connected to or used with the School's ICT systems unless approved in advance. Users must not try to install any software on the ICT systems without permission from the Business Manager. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.
The Business Manager is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.
Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

## Network access and security

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.
All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of the IT support team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Business Manager as soon as possible.
Users should only access areas of the school's computer systems to which they have authorised access.
When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.
Under no circumstances should a pupil be allowed to use a staff computer account.

**School Email**

Where email is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this acceptable use policy. The School's email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address.
The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.
- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.
- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).

- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible emails must not contain personal opinions about other individuals, e.g. other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

**Internet Access**

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use.
The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Business Manager and a red button message sent to Hi Impact.
Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.
Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.
Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the

disciplinary procedure.
If necessary such information may be handed to the police in connection with a criminal investigation.

## Digital cameras

The school encourages the use of digital cameras and video equipment; however staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to the school network as soon as possible.
- The use of mobile phones for taking photos of pupils is not permitted.

## File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

## Mobile Phones

Mobile phones are permitted in school, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. The school provides digital cameras/ipads for this purpose.
- All phone contact with parents regarding school issues will be through the school's phones. Personal mobile numbers should not be given to parents at the school.

## Social networking

The School has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.

- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the school's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Headteacher.
- Members of staff will notify the Business Manager if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).

## Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the Headteacher to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.
Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

## Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.
Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Headteacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.
The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

## ACCEPTABLE USE AGREEMENT

*To be completed by all staff*

As a school user of the network resources/ equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the school rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Business Manager.
I agree to report any misuse of the network to the Business Manager. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the Business Manager. I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Business Manager.
Specifically when using school devices: -

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.
I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

Signed ……. Date ……..

Print name ……

# School Technical Security Policy
# (Including filtering and passwords)

## Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

• users can only access data to which they have right of access.
• no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
• access to personal data is securely controlled in line with the school's Privacy Notice.
• logs are maintained of access by users and of their actions while users of the system.
• there is effective guidance and training for users.
• there are regular reviews and audits of the safety and security of school computer systems.
• there is oversight from senior leaders and these have impact on policy and practice.

As the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the E-Safety measures that might otherwise be carried out by the school itself (as suggested below). It is also important that the managed service provider is fully aware of the school E-Safety Policy /Acceptable Use Agreements). The school will also check the Local Authority / other relevant body policies / guidance on these technical issues.

## Responsibilities

The management of technical security will be the responsibility of Hi-Impact and their staff, and Dan Claire (IT Co-ordinator).

## Technical Security
## Policy statements

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 will receive guidance and training and will be effective in carrying out their responsibilities:

● School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
● There will be regular reviews and audits of the safety and security of school technical systems.
● Servers, wireless systems and cabling must be securely located and physical access restricted.
● Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
● Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
● All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually.
● Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (See Password section below).
• Hi-Impact and the school Finance Officer are 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

• Mobile device security and management procedures are in place.
• 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.
• Remote management tools are used by staff to control workstations and view users' activity.
• An appropriate system is in place for users to report any actual / potential technical incident to the E-Safety Co-ordinator/Headteacher or Finance Officer.
• An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school system.
• An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users.
• An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
• The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Privacy Notice Template in the appendix for further detail).

## Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

## Policy Statements

● All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually.
● All school networks and systems will be protected by secure passwords that are regularly changed.
● The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe.Consideration should also be given to using two factor authentication for such accounts. (We should never allow one user to have sole administrator access).
● Passwords for new users, and replacement passwords for existing users will be allocated by High Impact any changes carried out must be notified to the manager of the password security policy (above).
● All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
● Users will change their passwords at regular intervals – as described in the staff and pupil sections below.
● The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account.
● Requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for arequest by a pupil.

## Staff passwords:

● All staff users will be provided with a username and password by High Impact who will keep an up to date record of users and their usernames.
● Passwords are required to be 12 characters including 1 number
● must not include proper names or any other personal information about the user that might

be known by others
• the account should be “locked out” following five successive incorrect log-on attempts
• temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
• passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
● passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
Passwords cannot be reused for the previous 5 passwords and they must be changed every 180 days

- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
● should be different for systems used inside and outside of school.

## Training / Awareness

Members of staff will be made aware of the school’s password policy:
• at induction.
• through the school’s E-Safety policy and password security policy.
• through the Acceptable Use Agreement.

## Audit / Monitoring / Reporting / Review

The responsible person will ensure that full records are kept of:
• User Ids and requests for password changes.
• User log-ons.
• Security incidents related to this policy.

# St Joseph's Catholic Primary School

'Love one another as I have loved you' -John 15:12

# Privacy Notice Pupils and Parents

## Change History Record

| Version | Description of Change | Date of Policy Release by Judicium |
|---|---|---|
| 1 | Initial Issue | 06.05.18 |
| 2 | Updated for UK GDPR and international transfers outside of the UK | 06.05.21 |
| 3 | Added reference to sharing data section about Department for Education request for regular attendance data collection | 18.02.22 |
| 4 | Added reference to Biometric Data. | 19.08.22 |

This privacy notice describes how we collect and use personal information about pupils, in accordance with the UK General Data Protection Regulation (UK GDPR), section 537A of the Education Act 1996 and section 83 of the Children Act 1989.
Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

## Who Collects This Information?

St Joseph's Primary School is a "data controller." This means that we are responsible for deciding how we hold and use personal information about pupils and parents.
Under data protection legislation we are required to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.
It is important that you read this notice, together with any other policies mentioned within this privacy notice. This will assist you with understanding how we process your information and the procedures we take to protect your personal data.

## Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

## Categories of Pupil Information We Collect, Process, Hold and Share

We may collect, store and use the following categories of personal information about you:

- Personal information such as name, pupil number, date of birth, gender and contact information;
- Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses;
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- Attendance details (such as sessions attended, number of absences and reasons for absence);
- Performance and assessment information;
- Behavioural information (including exclusions);
- Special educational needs information;
- Relevant medical information;
- Special categories of personal data (including ethnicity, relevant medical information, special educational needs information);
- Images of pupils engaging in school activities, and images captured by the School's CCTV system;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Ni Number for the sole purpose of processing a claim for Free School Meals.

## Collecting this Information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. To comply with the UK General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.
It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

## How We Use Your Personal Information

We hold pupil data and use it for:

- Pupil selection (and to confirm the identity of prospective pupils and their parents);
- Providing education services and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Informing decisions such as the funding of schools;

- Assessing performance and to set targets for schools;
- Safeguarding pupils' welfare and providing appropriate pastoral (and where necessary medical) care;
- Support teaching and learning;
- Giving and receive information and references about past, current and prospective pupils, and to provide references to potential employers of past pupils;
- Managing internal policy and procedure;
- Enabling pupils to take part in assessments, to publish the results of examinations and to record pupil achievements;
- To carry out statistical analysis for diversity purposes;
- Legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with legal obligations and duties of care;
- Enabling relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- Monitoring use of the school's IT and communications systems in accordance with the school's IT security policy;
- Making use of photographic images of pupils in school publications, on the school website and on social media channels;
- Security purposes, including CCTV; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

## The Lawful Bases on which we use this Information

We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and
- The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is required or permitted by law.

## Sharing Data

We may need to share your data with third parties where it is necessary. There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it's the only way, we can make sure you stay safe and healthy, or we are legally required to do so.

We share pupil information with:

- the Department for Education (DfE) - on a statutory basis under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013;
- Ofsted;
- Other Schools that pupils have attended/will attend;
- NHS;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- Local Authority Designated Officer;
- Professional advisors such as lawyers and consultants;
- Support services (including insurance, IT support, information security);
- Providers of learning software such as [e.g., Timetables Rockstar, Edukey] and
- The Local Authority.

Recently the Department for Education have requested more regular data sharing on pupil attendance to help support those vulnerable and to assist with intervention strategies. Further information on how the Department for Education collects this data will be made available on the school website.

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

We do not share information about our pupils with anyone without consent unless otherwise required by law.

## Why we Share this Information

For example, we share students' data with the DfE on a statutory basis which underpins school funding and educational attainment. To find out more about the data collection requirements placed on us by the DfE please go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

## Storing Pupil Data

The school keep information about pupils on computer systems and sometimes on paper.

Except as required by law, the school only retains information about pupils for as long as necessary in accordance with timeframes imposed by law and our internal policy.

Full details on how long we keep personal data for is set out in our data retention policy, this can be found in the GDPR section on the school website.

## Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in limited circumstances.
Pupils will not be subject to automated decision-making, unless we have a lawful basis for doing so and we have notified you.

## Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the school only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.
Information about how we retain information can be found in our Data Retention policy. This document can be found on the school website.

## Security

We have put in place measures to protect the security of your information (i.e., against it being accidentally lost, used, or accessed in an unauthorised way).

## The National Pupil Database

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.
The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data?
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's education record, contact the Headteacher

## Requesting Access to your Personal Data

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.
If you want to request information, please see our Subject Access Request policy, for the procedures we take.

## Right to Withdraw Consent

In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Headteacher. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## Contact

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with the Headteacher in the first instance.
We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolve by the Headteacher, then you can contact the DPO on the details below:

| | |
|---|---|
| Data Protection Officer: | Judicium Consulting Limited |
| Address: | 72 Cannon Street, London, EC4N 6AE |
| Email: | dataservices@judicium.com |
| Web: | www.judiciumeducation.co.uk |
| Lead Contact: | Craig Stilwell |

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues at https://ico.org.uk/concerns.

## Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

# St Joseph's Catholic Primary School

# Privacy Notice Staff

'Love one another as I have loved you' -John 15:12

## Change History Record

| Version | Description of Change | Date of Policy Release by Judicium |
|---|---|---|
| 1 | Initial Issue | 06.05.18 |
| 2 | Updated for UK GDPR and international transfers outside of the UK | 06.05.21 |
| 3 | Added reference to Biometric Data | 19.08.22 |

This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).
Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.
It applies to all current and former employees, workers and contractors.

## Who Collects this Information?

St Joseph's is a "data controller." This means that we are responsible for deciding how we hold and use personal information about you.
We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.
It is important that you read this notice with any other policies mentioned within this privacy notice, so that you understand how we are processing your information and the procedures we take to protect your personal data.

## Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

## Categories of Information we Collect, Process, Hold and Share

We may collect, store and use the following categories of personal information about you:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment including references, proof of right to work in the UK, application form, CV, qualifications;
- Employment contract information such as start dates, hours worked, post, roles;
- Education and training details;
- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information;
- Details of any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- Information in your sickness and absence records such as number of absences and reasons(including sensitive personal information regarding your physical and/or mental health);
- Criminal records information as required by law to enable you to work with children;
- Your trade union membership;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals, performance reviews and capability issues;
- Details of your time and attendance records;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Details of your use of business-related social media;
- Images of staff captured by the School's CCTV system;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the School, you will be notified separately if this is to occur); and
- Details in references about you that we give to other;
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs.

## How we Collect this Information

We may collect this information from you in your application form, but we will also collect

information in a number of different ways. This could be through the Home Office, our pension providers, medical and occupational health professionals we engage with, your trade union, and even other employees. Information is also collected through CCTV, access control systems and any IT system the school has in place.

## How we use your Information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.
- When you have provided us with consent to process your personal data.

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.
The situations in which we will process your personal information are listed below:

- To determine recruitment and selection decisions on prospective employees;
- In order to carry out effective performance of the employees contract of employment and to maintain employment records;
- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- Enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management including retention, sickness and attendance;
- Performance reviews, managing performance and determining performance requirements;
- In order to manage internal policy and procedure;
- Human resources administration including pensions, payroll and benefits;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding;
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.
If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations.
We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is

compatible with the original purpose.

## How we use Particularly Sensitive Information

Sensitive personal information (as defined under the UK GDPR as "special category data") require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

We will use this information in the following ways:

- Collecting information relating to leave of absence, which may include sickness absence or family related leave;
- To comply with employment and other laws;
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;
- Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

## Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

## Sharing Data

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following:

- the Department for Education (DfE);
- Ofsted;
- Prospective Employers;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- LADO;
- Training providers;
- Professional advisors such as lawyers and consultants;
- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority;
- Occupational Health;
- DBS;
- Recruitment and supply agencies; and

Information will be provided to those agencies securely or anonymised where possible.
The recipient of the information will be bound by confidentiality obligations, we require them

to respect the security of your data and to treat it in accordance with the law.

## Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Once you are no longer a staff member at the school we will retain and securely destroy your personal information in accordance with our data retention policy. This can be found on the staff shared drive on Google in the policies/GDPR section and on the school website.

## Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found on the staff shared drive on Google in the policies/GDPR section and on the school website.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

## Your Rights of Access, Correction, Erasure and Restriction

Under certain circumstances, by law you have the right to:

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Headteacher in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

## Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Headteacher. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

We hope that the Headteacher can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolve by the Headteacher, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE

| | |
|---|---|
| Email: | dataservices@judicium.com |
| Web: | www.judiciumeducation.co.uk |
| Lead Contact: | Craig Stilwell |

## How to Raise a Concern

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

## Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

## Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an e safety issue or situation.

### Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

### Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

### Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

### Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

### Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

### Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

• Monitoring but not recording is also permissible in order to:
• Ascertain whether the communication is business or personal;
• Protect or support help line staff.
• The school reserves the right to monitor its systems and communications in line with its rights under this act.

### Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

### Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. Youtube).

### Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

### Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:
• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

### Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

### Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers,health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

### Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

### Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

### Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

### The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

### The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-andconfiscation

### The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems.

### The School Information Regulations 2012

Requires schools to publish certain information on its website: http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducingbureaucracy/requirements/changestoschoolinformationregulations

## Links to other organisations or documents

The following links may help those who are developing or reviewing a school E-Safety policy.

### UK Safer Internet Centre
Safer Internet Centre -
Childnet
Professionals Online Safety Helpline
Internet Watch Foundation

### CEOP
http://ceop.police.uk/
ThinkUKnow

### Others:
INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis
Netsmartz http://www.netsmartz.org/index.aspx

### Support for Schools

### Cyberbullying
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government Better relationships, better learning, better behaviour
DCSF - Cyberbullying guidance
DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies
Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org - http://www.cyberbullying.org/

### Social Networking
Digizen – Social Networking
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

### Curriculum
SWGfL Digital Literacy & Citizenship curriculum
Glow - http://www.educationscotland.gov.uk/usingglowandict/
Alberta, Canada - digital citizenship policy development guide.pdf
Teach Today – www.teachtoday.eu/
Insafe - Education Resources
Somerset - e-Sense materials for schools

### Mobile Devices / BYOD
Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note – BYOD

### Data Protection
Information Commissioners Office:
Your rights to your information – Resources for Schools - ICO
ICO pages for young people
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme
ICO Freedom of Information Model Publication Scheme Template for schools (England)
E-Safety Policy

ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO – Access Aware Toolkit
ICO - Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
SWGfL - Guidance for Schools on Cloud Hosted Services
LGfL - Data Handling Compliance Check List
Somerset - Flowchart on Storage of Personal Data
NEN - Guidance Note - Protecting School Data

### Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People
Kent - Safer Practice with Technology
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

### Infrastructure / Technical Support

Somerset - Questions for Technical Support
NEN - Guidance Note – Esecurity

### Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum
SWGfL BOOST Presentations - parents presentation
Connect Safely - a Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
DirectGov - Internet Safety for parents
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

## Glossary of terms

| | |
|---|---|
| AUP | Acceptable Use Policy – see templates earlier in this document |
| CEOP | Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes. |
| CPC | Child Protection Committee |
| CPD | Continuous Professional Development |
| CYPS | Children and Young Peoples Services (in Local Authorities) |
| FOSI | Family Online Safety Institute |
| EA | Education Authority |
| ES | Education Scotland |
| HWB | Health and Wellbeing |
| ICO | Information Commissioners Office |
| ICT | Information and Communications Technology |
| ICT Mark | Quality standard for schools provided by NAACE |
| INSET | In Service Education and Training |
| IP address | The label that identifies each computer to other computers using the IP (internet protocol) |
| ISP | Internet Service Provider |
| ISPA | Internet Service Providers' Association |
| IWF | Internet Watch Foundation |
| LA | Local Authority |
| LAN | Local Area Network |
| MIS | Management Information System |
| NEN | National Education Network – works with the Regional Broadband Consorti) to provide the safe broadband provision to schools across Britain. |
| Ofcom | Office of Communications (Independent communications sector regulator) |
| TUK | Think U Know – educational E-Safety programmes for schools, young people and parents. |
| VLE | Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting, |
| WAP | Wireless Application Protocol |