Trinity St Stephen First School E-Safety Policy

This policy has been developed by the Head teacher and consultations have taken place with the whole school community.

Policy approved by the governing body: 28 September 2015

Monitored by: The Head teacher

This policy will be reviewed annually.

This policy applies to all members of the school community (including staff, 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 Head teachers to such an extent as is reasonable to regulate 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. In the case of both acts, action can 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

Governors: The 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 receiving regular information about e-safety incidents and monitoring reports. The Child Protection Governor has taken on the role of E Safety Governor.

The role of the E- Safety Governor will include:

- Regular meetings with the Head teacher
- Regular monitoring of the E-Safety log
- Monitoring technical support to ensure appropriate filtering is in place
- Reporting in conjunction with the Head teacher to the Full Governing Body

The role of the Head teacher (supported by the Computing Subject Leader and the school Business Manager):

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The Head teacher and the Deputy Designated Officer (Kim Jones) are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See Appendix 1 – flow chart on dealing with e-safety incidents)
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety event taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with the school technical staff (through the School Business Manager)
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Technical Staff

At Trinity St Stephen First School technical support is bought in from the Local Authority and an independent provider.

The Business Manager liaises with the technical support team to ensure:

- That the school's technical infrastructure is secure and not open to misuse or malicious attack
- That the school meets required e-safety technical requirements and any Local Authority guidance that might apply
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

Teaching and Support Staff

The teaching and 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 (Appendix 2)
- They report any suspected misuse or problem to the Head teacher (in her absence the School Business Manager/ Deputy Designated Officer)
- 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 report immediately any miss-use
- Staff monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities 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 unsuitable material that is found in internet searches

Child Protection Officer

The 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 personal data
- Access to illegal/inappropriate material
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Extremism and radicalisation

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy (see Appendix 3)
- Need to have a good understanding of research skills
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be able to understand how to use mobile devices and digital cameras appropriately. 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

Parents/Carers

Parents and 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 parent's evenings, newsletters and the website. 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

Policy Statements

Education- pupils

Whilst regulation and technical solutions are important the pupils must also be taught to take a responsible approach. The education of e-safety in all areas of the curriculum is an essential part of the school's e-safety provision.

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 the computing curriculum and should be regularly revisited
- E-safety messages should be reinforced as part of assemblies and other school activities
- Pupils should be taught to be critically aware of material they find on the internet
- Pupils should be taught to acknowledge the source of their information
- Staff should always act as good role models for children in their use of digital technologies, the internet and mobile devices
- Staff should ideally direct children to safe sites whilst searching the internet. If children are freely searching staff should be vigilant in monitoring the content of the websites visited

Education- parents/carers

The school takes its role as an educator of parents and carers in e-safety seriously and endeavours to provide up to date information and support through newsletters, information sessions and references to helpful websites.

Education and 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:

- All new members of staff will be given the E-safety Policy as part of the Staff Handbook.
- The Head teacher will revisit the policy regularly with the staff and training needs will audited and training provided where necessary.

Technical – infrastructure

- The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures within this policy are implemented. The school will need to ensure that the provider of technical support is fully aware of this policy.
- 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 safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password. Users are responsible for the security of their usernames and passwords
- The administrator passwords for the school used by the Network Manager (independent technical support) must be available to the Head teacher and kept in the school safe
- The School Business Manager 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

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. All members of our school community need to be aware of potential harm caused by uploading images onto the internet
- The school will inform and educate pupils and parents/carers about the risks associated with sharing and distributing images
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos/ pictures of their children at school events for their own personal use. For everyone' s protection these must not be shared on social media sites

- Staff are allowed to take images to support learning. These images must not be shared and must only be taken on school equipment
- Photographs taken at school events or during school time must be used appropriately and never have full names that can be linked to individuals. Written permission from parents or carers will be obtained before photographs are published. (Appendix 3)

Data Protection

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

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

The school ensures that:

- It will hold 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 is made to ensure data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be obtained fairly
- The school follows guidance from RBWM on Data Protection (See Appendix 4)
- It is registered as a Data Controller for the purposes of the Data Protection Act

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 (ie First Class)

Communications

The school email service (First Class and Microsoft 365) may be regarded as safe and secure and is monitored. All users should be aware that email communications are monitored

Users must immediately report, to the Head teacher, the receipt of any communication that makes them feel uncomfortable is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

Any digital communication between staff and students, pupils or parents/carers, school and any other school or business must be professional in tone and content. Communications must only take place on official school systems. Personal email addresses, text messaging between personal devices and social media must not be used for these communications

The use of personal mobile devices is restricted in school to the Staff Room, the upstairs PPA room, the School Office and outside in the school car park. Mobile devices should be kept, out of sight with other personal belongings- this maybe in a classroom cupboard or a school locker. Under no circumstances should mobile phones or devices be visible or in use in any areas populated by children. Mobile devices should only be accessed during non-teaching times

Social Media

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools 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 the risk of harm to pupils, staff and the school through limiting access to personal information:

- Training
- Clear reporting guidance
- Risk assessment, including legal risk

School staff must 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 the risk of loss of personal information.

This policy has been written using material from South West Grid for Learning

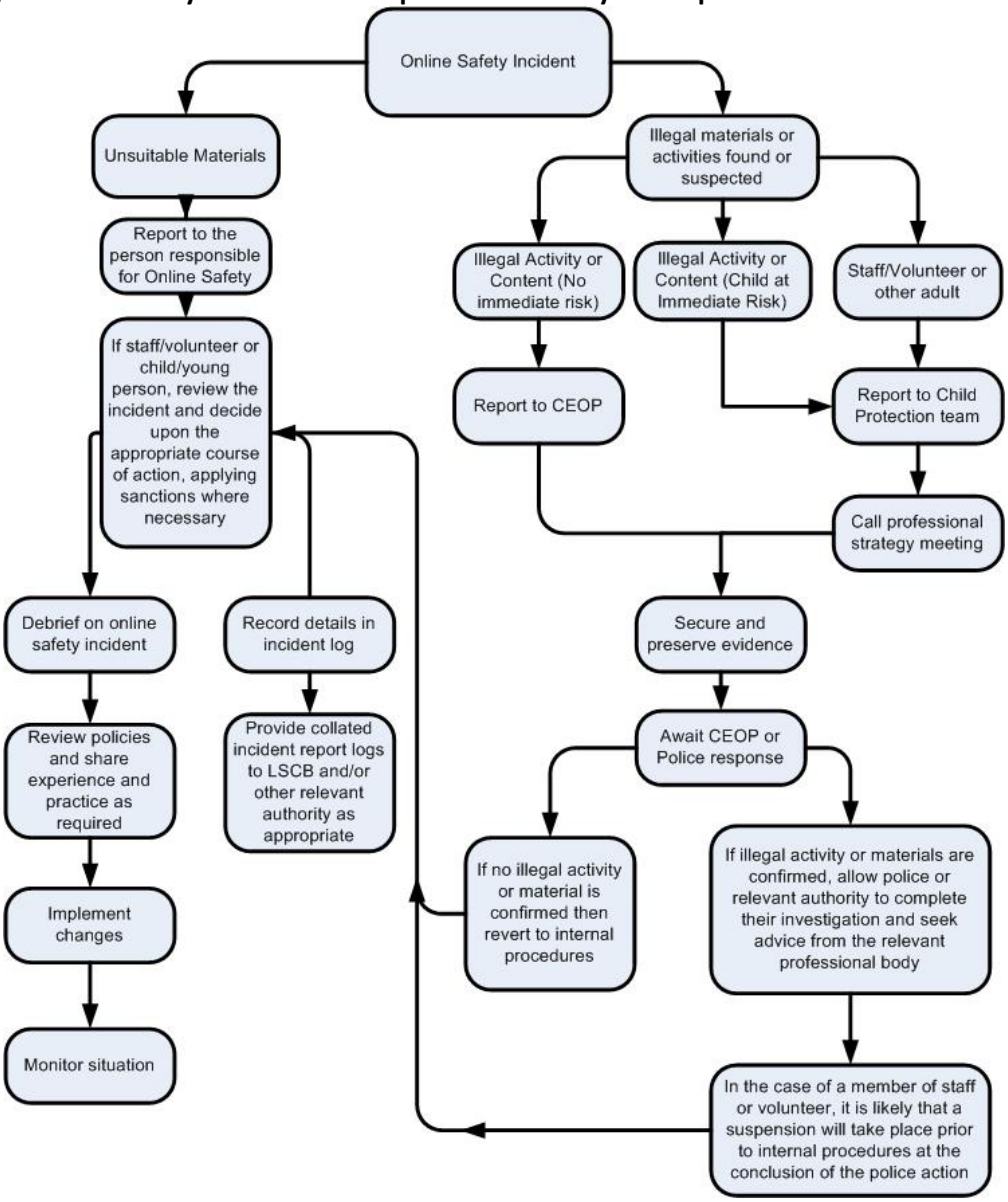
Appendix 1

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). SWGfL BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool)

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.



Appendix 2

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

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

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

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

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

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

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

Staff / Volunteer Name	
Signed	
Date	

Appendix 3

Pupil Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

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): ……..

Appendix 4

Royal Borough of Windsor and Maidenhead

STANDARD PHOTOGRAPHY, VIDEO AND VOICE CONSENT FORM

RBWM confirms that it shall only use photographic/video images of young people in line with the Information Commissioner's Office Code of Practice to demonstrate or promote activities and events relating to schools and curricula provision. A copy of the Code of Practice can be obtained from ICO at www.ico.gov.uk.

Please complete the form and, where appropriate, ensure your child is aware of your decision.

Child's surname	Child's forename	Child's class

Area where images may be used	Use of Image	Use of name
School Prospectus – may contain photographs of pupils individually or in groups.	**YES** / NO	Names are not used
School Newsletter - includes articles and information about school activities and events. Names may appear in text and could be used to identify individual pupils.	**YES** / NO	**YES** / NO
School Display boards and notices – photographs may include individual or groups to demonstrate, promote or congratulate pupils and their work.	**YES** / NO	Names are not used
School and RBWM Web Sites – Visitors to web sites may view, on line, information on a wide range of events and activities promoting the school/RBWM.	**YES** / NO	Names are not used
School Web Sites – We celebrate children's achievements in our monthly newsletter, and publish this on the school's website. We hope you will consent to using publishing your child's first name in this way.	Images are not used	**YES** / NO
Local and National Press coverage – features school/RBWM events and activities. Names may appear in text and could be used to identify individual pupils.	**YES** / NO	**YES** / NO

*Answers will be taken to be **YES** unless otherwise indicated*

Under the Data Protection Act and for internal identification purposes only, a photograph of all pupils and staff are kept on the schools database.

RBWM/School cannot be responsible where members of the public take photographs/videos at activities and events which involve school pupils or control how they are stored or subsequently used. This includes the publication on social networking or personal storage websites and mobile phones. We do request that this does not happen.

- **This consent will be deemed to apply for the entire time my child attends Trinity St Stephen School**. (Please delete the previous sentence if you would like to give consent annually instead)
- I understand that I may withdraw my consent at any time by contacting the school and that, where possible, any publications or material containing the image/voice of my child will be recalled and withdrawn.
- I confirm that I have read and agree to the terms contained within this Consent Form.

Parent/Carer Signature…… Date: …… / …… /

Parent/carers name:……(Please print)

1. General

1.1 This guide aims to outline the obligations of a school under the Data Protection Act 1998 (the Act) when processing personal data.

1.2 Further detailed information is available from the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 0303 123 1113
Fax: 01625 524510

1.3 A school is a Data Controller and must nominate an individual as their Data Protection Officer. This person will be the contact for the Information Commissioner's Office and will be named on the school's Data Protection Notification register entry.

1.4 The Data Controller is responsible for compliance with its Data Protection Act 1998 obligations.

1.5 A data subject is an identifiable living individual (e.g. student, parent, teacher, governor)

1.6 Breaches of the Data Protection Act 1998 can lead to individuals receiving a criminal record.

1.7 Notification is an annual activity which costs £35 (rising to £500 if the school employs 250 or more members of staff). Failure to submit and keep updated the school's Notification is a breach of the Data Protection Act 1998.

1.8 Comprehensive procedures must exist covering all personal data processing undertaken in school and any exchanges or sharing of personal data with other organisations.

For additional advice contact Martin Tubbs (martin.tubbs@rbwm.gov.uk) or Jennifer Shaw (jennifer.shaw@rbwm.gov.uk) RBWM's qualified Data Protection Officers.

2. **The Eight Principles**

2.1 When processing personal data the school must comply with the eight Data Protection Principles.

A summary of the principles and what is required is listed below.

1. Fair & Lawful (plus schedule 2 & 3)

Before processing begins the school must tell the data subjects (people whose information will be processed) who the Data Controller is for the information. The school must also satisfy itself that it has a Schedule 2 condition and in the case of sensitive personal information a Schedule 2 **and** a Schedule 3 condition.

Personal data processing should only be for specified and lawful purposes.

This means that the school must be clear about why processing of the personal data is needed. (Refer to Privacy Notice Guidance). The school must tell people **all** of the ways in which personal information will be used and the information must **only** be used for those purposes.

2. Adequate, relevant, not excessive

The processing of personal data should involve only those details required to meet the purpose of the processing, no more, no less.

3. Accurate & up to date

The personal data processed should be accurate & (if necessary) up-to-date. This means the school must be proactive in encouraging data subjects to review their personal data and ask them to inform the school of any changes. Notification of changes must be implemented immediately. The school should have proper procedures to ensure this happens.

4. Not kept for longer than necessary

The school should have an up to date retention and disposal policy for the personal data it processes. Guidance for schools if available here:

http://www.irms.org.uk/resources/848

The Information Commissioner's Office expects this guidance to be followed.

5. In accordance with data subject rights

This means that data subjects have the right to see the personal information held by a school which is about them. The school must comply with such a request within 40 calendar days. Importantly if the school is closed for holidays, the clock stops.

This right may be denied under certain circumstances, for example, if there is an ongoing criminal investigation involving a data subject which might be compromised by disclosure.

There are two distinct rights to information held by schools about pupils:

1) The subject access right – under the Act a pupil (usually aged over 12) has the right to a copy of their own information. In certain circumstances requests may be made by a parent on behalf of their child (for example if the child is under 12).

The maximum charge for this service is £10

2) Rights to the educational record – under the Education (Pupil Information) (England) Regulations 2005, a parent has the right to access their child's educational record. The maximum charge for this service is £50.

Under the subject access right, parents will only be able to see all the information about their child when their child is unable to act on their own behalf or give their consent.

6. Technical and Organisational Security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In practice, it means the school must have implemented appropriate security measures to prevent personal data being accidentally or deliberately compromised. This includes both physical measures, such as locked doors/cabinets, technical measures, such as computer firewirewalls/passwords and, just as importantly, comprehensive procedures and properly trained staff.

7. No transfers outside EEA without safeguards

The EEA (European Economic Area) all abide by common principles/standards for the processing of personal data. Before any personal data can be processed outside the EEA the school must have a contract in place that will ensure the same protections that the eight principles embody are in place.

In reality it is unlikely that a school would have a need to process any personal data outside the EEA.

3. Conclusion

- Nominate a Data Protection Officer
- Ensure staff are properly trained
- Have up-to-date procedures for dealing with personal data processing, including receiving and responding to subject access requests
- Ensure adequate security measures are employed and have a comprehensive procedure for dealing with security breaches
- Ensure annual notification is completed and kept up-to-date

- Publish and/or provide comprehensive Privacy Notices

- Remember breaches of the Data Protection Act 1998 can lead to a criminal record and fines of up to £500,000

- - - - - - - - - - - - - - - - o - - - - - - - - - - - - - - - - o - - - - - - - - - - - - - - - -

Appendices

a) Privacy Notice

b) Schedule 2

c) Schedule 3

d) Sensitive Personal Data

Appendix a)

Privacy Notice

It is a requirement of the Data Protection Act 1998 that **before** any personal information processing begins a Privacy Notice is published for those people affected by the processing.

A Privacy Notice is required regardless of whether personal information is to be stored on a computer or not.

This guidance sets out what information has to be included in a Privacy Notice and how it can be provided.

The Information Commissioner's website states:

> You will need to outline what and how information is going to be processed. This is to make sure the individual knows exactly what is going to happen to their information and how it is going to be used. You shouldn't be doing anything with personal information unless the individual is made aware (unless certain exemptions apply)

In practice this means that whenever you request any personal information, usually via an application form or on a website page, you must state **all** the purposes for which the data is required.

It is not acceptable to use general terms to describe the purposes so do not be tempted to use phrases like "Any processing the school needs to undertake".

Information about processing must be presented in the same typeface and font size predominantly used elsewhere on the data collection form.

Do not incorporate Privacy Notice information in the 'small print' - it is not acceptable.

Within the Data Protection Act 1998 people are referred to as data subjects. A data subject has a right to ask for and receive a copy of the information an organisation holds about

them. In order for them to be able to do this they need to be given information in the Privacy Notice about how to exercise that right. For this reason it is good practice to separate the Privacy Notice from that part of an application form which has to be completed and returned to us. Doing so means that the data subject is able to retain the information they need about the processing and how to exercise their access right.

The information to include is:

You have a right to request and receive a copy of the information the school holds about you.

To exercise this right please write to:

Mrs Louise Lovegrove

A layered approach to a Privacy Notice is preferable:

The top level comprises a brief summary of the processing and is included on the Privacy Notice.

The next level containing more detail should be published on your website.

The third level includes a link to the full text of the Data Protection Act 1998.

If you have any queries about Privacy Notices that your school Data Protection Officer cannot help you with, then please contact the Data Protection Officer at RBWM Town Hall.

Appendix b)

Schedule 2

In order to legitimise the processing of personal information, the school must be able to meet a condition in Schedule 2:

1 The data subject has given his consent to the processing (Do not rely on this condition – contact RBWM's Data Protection Officer for guidance)

2 The processing is necessary—

(a) for the performance of a contract to which the data subject is a party, or

(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

If sensitive personal information is being processed, a further condition in Schedule 3 must also be met.

Appendix c)

Schedule 3

In order to legitimise the processing of sensitive personal information, the school must be able to meet a condition in Schedule 3 (in addition to a condition in Schedule 2):

1 The data subject has given his explicit consent to the processing of the personal data. (Do not rely on this condition – contact RBWM's Data Protection Officer if advice regarding this is required)

2 (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3 The processing is necessary—

(a) in order to protect the vital interests of the data subject or another person, in a case where—

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing—

(a) is carried out in the course of its legitimate activities by anybody or association which—

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6 The processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7 (1) The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8 (1) The processing is necessary for medical purposes and is undertaken by—

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9 (1) The processing—

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10 The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Appendix d)

Sensitive Personal Data:

Personal data consisting of information as to –

(a) the racial or ethnic origin of the data subject

(b) his political opinions

(c) his religious beliefs or other beliefs of a similar nature

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992

(e) his physical or mental health condition

(f) his sexual life

(g) the commission or alleged commission by him of any offence or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

- - - - - - - - - - - - - - - - - o - - - - - - - - - - - - - - - - - o - - - - - - - - - - - - - - - - -