eSafety Policy

Reviewed by (Headteacher/DSL):

Date: April 2021

Approved by Headteacher:

Review Date: April 2022

Page left blank intentionally

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

Bristol Steiner School eSafety Policy

1. Rationale
Bristol Steiner School (BSS), understands its responsibility to educate staff, children and families in eSafety issues. For a number of reasons which go beyond the scope of this policy statement, BSS, like all Steiner schools, chooses not to use computers as a learning tool with pre-adolescent children. But we do recognize that use of computers plays an important in modern life and that pupils need to be helped to develop appropriate skills and a healthy attitude to their use as well as a good understanding of how the technology works. This entails teaching appropriate behaviours and critical thinking to enable users to remain both safe and legal when using the internet and related technologies. Our eSafety policy also recognizes the importance of ensuring that our online systems are safe and secure and are committed to being proactive and responsive to cyber risks.

Our eSafety policy is an essential part of our Safeguarding practice. BSS is committed to safeguarding and promoting the welfare of young people and vulnerable adults. We believe the welfare of the child is paramount and that no child should suffer harm of any form, either at home or at school. Everyone who works at or visits our school has the responsibility to make sure all our children are safe.

For the purposes of this policy, 'staff' also includes agency staff, volunteers, and pupils working in our Schools, and 'parents' includes carers and legal guardians – unless this is clarified further within the text.

2. Aims
This e-Safety policy aims to clarify the responsibilities of management and staff and services users when using information technology within the School, to safeguard children's welfare in relation to the above areas and minimize the risk of harm and to fulfil legal duties in relation to personal data and other areas. The School aims to create a safe e-learning environment that:

- ensures the School fulfils its duty of care to pupils; and
- provides clear expectations for staff and pupils on acceptable use of the internet.

3. Definitions
Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using include:

• Websites
• Learning Platforms and Virtual Learning Environments
• Email and Instant Messaging
• Chat Rooms and Social Networking
• Blogs and Wikis
• Podcasting
• Video Broadcasting
• Music Downloading
• Gaming
• Mobile/Smart phones with text, video and/or web functionality
• Other mobile devices with web functionality

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

This policy is inclusive of both fixed and mobile internet; other technologies such as PCs, laptops, mobile phones, camera phones, webcams, digital video equipment and and portable media players.

4. Leadership

The e-Safety Officers for the School will be the Headteacher and the DSL. The duties of the Headteacher/eSafety officer are:

- reviewing the eSafety policy and procedures;
- providing the first point of contact and advice for School staff, trustees, pupils and parents about eSafety matters;
- liaising with the School's IT supplier to ensure they are kept up to date with e-Safety issues and to advise of any new trends, incidents and arising problems to the Senior Management Team (SMT) and trustees;
- raising the profile of e-Safety awareness with the School by giving advice and ensuring access to training and relevant E-Safety literature when appropriate;
- ensuring that all staff are aware of eSafety policies at Induction and in particular the procedures that need to be followed in the event of an E-Safety incident taking place;
- maintaining a file of internet related incidents and co-ordinate any investigation into breaches; all incidents must be recorded using a Safeguarding Concern form;
- meeting regularly liaising with the SMT and Trustees to discuss current issues and review incident logs;
- liaising with the Local Authority and other eSafety meetings as necessary; and
- assessing, as far as is reasonably practicable, the impact and risk of emerging technology (eg. a new social networking website).

These duties may be delegated to the Admin Manager as appropriate.

5. Implementation

This policy is the responsibility of everyone who works at, volunteers for or visits BSS. The eSafety officers, will ensure that arrangements will be made to bring this policy to the notice of all staff (including new, temporary, and part-time employees), agency and other contract staff, volunteers, visitors and pupils during Induction and throughout their time at the School so that they fulfill their duties to co-operate with this policy. Staff receive regular information and training on e-Safety issues through the eSafety coordinator at staff meetings and sign the Acceptable Use Agreement (see Code of Conduct policy). They should familiarize themselves with the Description of ICT Applications informs of risks and benefits. This policy and procedure will apply in all these contexts, including school activities taking place offsite. BSS expects services delivered by partner organisations to have safeguarding procedures in place. This policy should appear on the School website.

6. Other policies

This policy works in conjunction with the following School related policies and procedures:

1. *Anti-bullying*
2. *Behaviour*
3. *Code of conduct (staff)*
4. *Complaints/Concerns/Grievance*
5. *Curriculum*
6. *Equalities*
7. *Health and Safety*
8. *Parent Handbook*
9. *Parent Prospectus*

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

10. Staffing
11. Safeguarding and Child Protection

7. Monitoring and Review
BSS will seek to continually improve all its related safeguarding policies, procedures and guidelines including eSafety. BSS will review this policy on a regular basis to confirm that content and approach is still appropriate. The review will take place whenever there are significant changes and not later than 12 months from the previous review date. This eSafety policy is very much a work in progress and will need to be evolved in the light of experience. As Tolstoy said about money, computers 'are a good servant but a bad master'.

8.Law and Guidance
This policy complies with the Data Protection Act 1998 and Freedom of Information Act.

9. Safe Systems
The School is committed to ensuring that all its ICT systems are as secure as possible. The suppliers of the hardware and software of the School's computer network provide on-going technical support and advice to help maintain eSafety. The School will ensure that:

- ICT systems capacity and security will be in place, inlcuding an effective firewall, anti-virus software; username and password protected areas for staff; filtering software for search engines and browsers to protect pupils and staff, and a technical support line for instant response to technical issues;
- derived materials by staff and pupils complies with copyright law;
- eSafety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them;
- personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act;
- all reasonable precautions will be taken to prevent access to inappropriate material.

However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer. The School does not accept liability for the material accessed, or any consequences of Internet access. The School will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

10. Curriculum
Children must be made aware of the risk associated with IT. The risks associated with use of ICT by children can be grouped into the following categories:

- Content: exposure to inappropriate images, pornography, information advocating violence, racism or illegal and anti-social behaviour that cannot be evaluated in a critical manner.
- Contact: chat rooms, social networking sites, adults seeking to gain the trust of young people ("grooming") with a view to sexually abusing them and risk of cyber-bullying and disclosing personal information (addresses, mobile numbers, photos, etc.)
- Commerce: vulnerability to unregulated commercial activity, potentially resulting in serious financial consequences for themselves and parents and vulnerability to fraud or identity theft.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- Culture: involvement in inappropriate, anti-social or illegal activities or exposure to unsuitable materials or inappropriate social networks using information in a way which breaches copyright laws.

Pupils using ICT in lessons must sign the ICT Parent Consent Form and Pupil Declaration (see Appendices).

11. Computer/Internet Addiction.
Children are prone to computer addiction which can have a negative impact on their health, social, emotional development and their educational attainment. Studies have established recurring links between computer addiction and depression. It disrupts sleeping patterns, takes away from time spent outdoors and being generally physically active. For young children, in particular this can lead to significant developmental issues. The DSL will make pupils aware of these dangers by briefing children during lessons and assemblies. The DSL should be informed if there is a concern that pupils may be experiencing this at home.

12. Responding to Incidents
This eSafety policy seeks to reduce risks but it cannot eradicate online risk entirely. The School cannot accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment and to keep online security up to date. All incidents, whether involving pupils or staff, must be recorded using a Safeguarding Concern Form and reported to the DSL. The Headteacher/eSafety officer should periodically review with the DSL the Safeguarding record file for evidence of emerging patterns of individual behaviour or weaknesses in the School's eSafety systems. This information should be used to update the E-Safety policy.

13. Inappropriate websites
Where there has been unintentional access of inappropriate websites, teachers should:
- reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the eSafety message;
- reported to the eSafety Coordinator and details of the website address and URL provided; and
- the Headteacher should liaise with the Business Manager to ensure that access to the site is blocked and the school's filtering system updated.

Where there has been Intentional access of inappropriate websites by a pupil, teachers should:
- sanction the pupil in accordance with the Behaviour policy;
- report the incident to the eSafety coordinator and details of the website address and URL recorded;
- the E-Safety coordinator should liaise with the Business Manager to ensure that access to the site is blocked; and
- inform the pupil's parents of the incident.

14. Inappropriate use of ICT by staff.
If a member of staff witnesses misuse of ICT by a colleague, they should report this to the Headteacher/eSafety officer. The Headteacher/eSafety officer should notify the Admin Manager so that the computer or laptop on which the misuse was witnessed. The Headteacher/eSafety officer should arrange with the Admin Manager to carry out an audit of use to establish which user is responsible and the details of accessed materials. Once the facts are established, the Headteacher should follow the Disciplinary Policy Procedure

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

against the staff member and report the matter to the Trustees and the police where appropriate. The incident to the police and follow their advice, which should also be recorded on Safeguarding concern form.

15. Mobile Phones and laptops

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. Mobile phones may be used as long as their use is appropriate. The use of a mobile phone by staff and other professionals must not detract from the quality of the supervision and care of children. Appropriate use is defined as follows:

a. NOT permitted

- Staff will not have their private mobile phone on their person during work hours.
- Mobile phones and other photographic devices will be kept in a secure area away from where the children are accommodated.
- Staff may use their mobile phones during their designated breaks and in an area away from the children.
- The School's contact number will be given as an emergency number in case practitioners need to be contacted.
- Staff are not to use any mobile phone cameras to photograph the children.
- Staff need to ensure that visitor's phones are not used in the School.
- Parents and visitors will be asked to hand in their mobile phones to the School Office whilst on site.
- Staff must never exchange mobile phone numbers with parents in their School (unless there is a specific purpose as stated below).
-

b. Permitted use

- Use of mobile phones will be for business and emergency purposes and practitioners are not to be distracted from the care of children.
- Staff will be held responsible for the content and security of their own phones, e.g. access to web pages. If this is deemed to be a safeguarding issue this will be dealt with in line with the Schools Safeguarding and Child Protection and Staffing policies.
- Images taken of the School or its children should be downloaded onto the School's computer/laptop only. Images must not be downloaded onto any personal computer.
- Offsite on outings, mobile phones may be very useful. Where parent information is stored on a personal mobile for an outing this needs to be deleted after the outing is over. It is recommended for the senior member of staff to record this occurrence. Alternatively paper information may be taken on outings.
- Some professionals (e.g. childminders) who visit the School on a regular basis can use mobile phones and other devices in groups, as long as any phone calls are kept as brief as possible so as not to detract from the quality of supervision of the children.
- All professionals should be reminded that that phone cameras, and photographs in general, can be used inappropriately, and the DSL or other staff will supervise and may veto, if necessary, the use of any mobile phone or camera within the vicinity of children on the School's premises. All professionals should seek permission from parents to take photographs of their children's learning journey, and make it clear to them how they take and share those photographs with parents, whether by mobile phone or by camera.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

It is against School policy for pupils to use mobiles in School. In terms of eSafety, most modern mobiles (Smartphones, iPods etc.) have internet connectivity which would give unregulated private internet access only to certain pupils. If a mobile is heard or any pupils are seen using a mobile (or similar) anywhere on the school site it will be confiscated for the remainder of the day and possibly longer depending on the nature of the incident. For the same reason**, unless a pupil has obtained special permission to bring in their laptop for school work**, any laptops found being used at School will also be confiscated. Pupils posting images, comments, sound recordings, videos or any other material pertaining to any staff member, trustee, pupil, parent or anyone with a connection to the school on websites, YouTube, Facebook or any other social networking sites will be dealt with under the Behaviour Policy.

16. E-mail
E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of E-Safety. Unprofessional use of email can pose a risk to the School.

The School will ensure that:
- Staff are aware that access in the School to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on the School's headed paper.
- Chain letters, spam, advertising and all other e-mails from unknown sources will be deleted without opening or forwarding.

17.e-Communication between Staff and Pupils
Staff must not email pupils from private email accounts. Only School email accounts should be used. Emailing between staff and pupils should only be for assistance with schoolwork or other official school-related business. Texting between staff and pupils is not allowed except in an emergency situation on a class trip which has been risk assessed. It is against school policy for staff Facebook users to add current pupils as friends or accept friendship requests from pupils or ex-pupils under 18 years of age. Staff found to contravene these E-Communication guidelines could face a disciplinary hearing.

18. Social Networking and communication
Social networking Internet sites (such as Snapchat, Twitter, Facebook) provide facilities to chat and exchange information online, but the online world is very different from the real one with the temptation to say and do things beyond usual face to face contact. The School will ensure that:
- all staff are aware that use of social networking sites and newsgroups in School is not allowed and will be blocked/filtered;
- parents, children and staff will be advised of the dangers of discussing children, staff or the School on social networking sites;
- Trustees will consider taking legal action, where appropriate, to protect children and staff against cyber bullying and defamatory comments;
- video conferencing will only be used if risk asses.

19. Digital/Video Cameras
Pictures, videos and sounds are not directly connected to the Internet but images are easily transferred. The School will ensure that:

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content';
- parents will not use digital cameras, mobile phones or video equipment at the School unless specifically authorised by staff;
- the Headteacher or nominee will inform parents and others present at events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

20. Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the School is allowed.

21. Published Content and the School Website

The School's website is a valuable source of information for parents and potential parents but it must be managed to reduce any potential risks to families. The School will ensure that:

- contact details on the Website will be the School's address, e-mail and telephone number;
- staff and children's personal information will not be published particularly children's names in association with photographs;
- the eSafety Coordnator or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate;
- photographs and videos that include children will be selected carefully and will not enable individual children to be clearly identified and consent from parents will be obtained before photographs of children are published on the School's website;
- work can only be published with the permission of the child and parents;
- parents may upload pictures of their own child only onto social networking sites; if the picture includes another child/children then it is their responsibility to gain permission from that child's parents;
- the Trustees may ban the use of photographic equipment by any parent who does not follow the School's policy.

22.Parents

All parents should be asked to sign 'Parent and Pupil consent to ICT' along with pupils (see Appendices). They should be asked their permission and decide as to whether they consent to images of their child being taken/used on the School's publicity, including the website. Parents will be asked to sign the Acceptable Use of IT Agreement if they use the internet in the School along with staff (see Appendices). They should be made aware of useful information and links to sites like Thinkuknow, Childline, CEOP and the CBBC Web Stay safe page, and other e-Safety information through newsletters, the website, and the prospectus sent out by the School to help keep their children safe. Parent training in helping keep children safe online should be considered.

23. E-Safety Complaints

Complaints of Internet misuse will be dealt with by the Headteacher. Complaints involving a safeguarding concern shall be dealt with in accordance with the School's Safeguarding procedures. Parent/carers will be informed of the complaints procedure.

24. Appendices

1. Description of ICT Applications
2. ICT Pupils' Code of Conduct

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

3. Data policies: Data protection, Data Management, Data Transit, Emailing Confidential Documents, Email Policy & Procedure , Photographs, ‘Use your camera and video courteously’
5. ICT Parent Consent Form and Pupil Declaration

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

Description of ICT applications: Benefits & Risks

Technology / Application	Description / Usage	Benefits	Risks.
Internet	• Enables the storage, publication and retrieval of a vast range of information • Supports communication systems	• Provides access to a wide range of educational materials, information and resources to support learning • Enables pupils and staff to communicate widely with others • Enhances schools management information and business administration systems	• Information is predominantly for an adult audience and may be unsuitable for children. • The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information • Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites
Email	• Allows written communications over the network and the ability to attach documents	• Enables exchange of information and ideas and supports collaborative working • Enhances written communications skills • A good form of communication for children with some disabilities	• Difficulties controlling contacts and content • Use as a platform for bullying and harassment • Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems • Hacking • Unsolicited mail

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

‘.**chat/ instant messaging**	• Chat rooms allow users to chat on-line in real time in virtual meeting places with a number of people • Instant messaging allows real-time chat for 2 people privately with no- one else able to join. Users have control over who they contact through ‘buddy lists	• Enhances social development by allowing children to exchange experiences and ideas and form friendships with peers. • Use of pseudonyms protects the child’s identity • Moderated chat rooms can offer some protection to children.	• Anonymity means that children are not aware of who they are really talking to. • Chat rooms may be used by predatory adults to contact, groom and abuse children on-line • Risk of children giving away personal information that may identify or locate them • May be used as a platform to bully
Technology / Application	**Description / Usage**	**Benefits**	**Risks**
Social Networking Sites	• On-line communities, including blogs and podcasts, where users can share text, photos and music with others by posting items onto the site and through messaging • It allows creation of individual profiles • Users can develop friends lists to allow access to individual profiles and	• Allows children to network with peers and join forums to exchange ideas and resources • It provides a creative outlet and improves ICT skills	• Open access means children are at risk of unsuitable contact. • Risk of children posting unsuitable material on-line that may be manipulated to cause them embarrassment or distress • Children may post personal information that allows them to be contacted of located • May be used as a platform to bully or harass

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

	invite comments		
File sharing (peer to peer networking)	• Allows users to share computer capability, networks and file storage • Used to share music, video and other materials	• Allows children to network within a community of peers with similar interests and exchange materials	• Illegal download and copyright infringement • Exposure to unsuitable or illegal materials • Computers are vulnerable to viruses and hacking.
Mobile phones and multi-media equipment	• Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email	• Provides children with a good means of communication and entertainment. • They can also keep children safe and allow them to be contacted or stay in contact	• Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging. • Risk from violent crime due to theft • Risk of cyberbullying via mobile phones.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

ICT Pupils' Code of Conduct
(Also recommended for out of School use)

- Pupils are expected to behave responsibly when using the school's ICT facilities including the internet, just as they are expected to do so in a classroom or other school area - general School rules still apply
- The ICT facilities are expensive and must be treated with great care
- The internet is provided for educational purposes so that:
    - Pupils can enhance their learning and research skills
    - Pupils with disabilities can overcome educational difficulties
    - Pupils can gain basic fluency and confidence when using the internet.
- Access is a privilege, not a right – and can be rescinded
- Individual users of the internet are responsible for their behaviour and communication over the network

To ensure the E-safety of ALL pupils the following are <u>not</u> permitted:

- Disclosing your assigned network password to other pupils or anyone else
- Using other pupils' network passwords
- Trespassing in other pupils' folders, work or files
- Violating copyright laws, especially the illegal copying of software
- Intentionally wasting limited resources, such as server processing time, ink and paper
- Sending or displaying offensive messages or pictures
- Sending junk mail
- Revealing your photograph, phone number of other personal details on web pages or in emails without written parental and school permission
- The use of the internet to buy, sell or advertise
- The participation in chat rooms or newsgroups except where these are educational and supervised by a member of staff
- Post to/read sites such as Twitter, Facebook, blogs, etc. during School hours
- Subscribe to internet mailing lists without specific permission from the supervising ICT Teacher in each case

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

Data management – Data Protection Policy & Procedure

Data protection law reinforces common sense rules of information handling, which most organisations try to follow anyway. It is there to ensure that organisations manage the personal information they hold in a sensible way. Organisations must keep the information accurate and up to date, they must only keep it for as long as they need it for a specified purpose and they must keep it secure.

"Data" is information that can be stored either on equipment (i.e. computer) or physically (i.e. in a filing system), or is information that forms part of an accessible record.

Bristol Steiner School Data Protection Policy

The school will comply with:

- The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.
- Information and guidance displayed on the Information Commissioner's website (www.dataprotection.gov.uk).
- This policy should be used in conjunction with the school's Internet Use Policy & the Data in Transit Policy.

The Data Protection Act 1998 sets out eight protection principles which form the legislative framework and with which a data controller must comply.

1st: Personal data shall be processed fairly and lawfully.

2nd: Personal data shall be obtained only for one or more specified and lawful purposes.

3rd: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4th: Personal data shall be accurate and, where necessary, kept up to date.

5th: Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

6th: Personal data shall be processed in accordance with the rights of data subjects under the Act.

7th: 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.

8th: Personal data shall not be transferred to a country or territory outside the European Economic Area…

Data Gathering

- All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.
- Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

Data Storage

- Personal data will be stored in a secure and safe manner.
- Electronic data will be protected by standard password and firewall systems operated by the school.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting in the office.
- Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
- Particular attention will be paid to the need for security of sensitive personal data.
- Teachers who may need to work on children's files at home will remove any identifiable information to protect the identity of individual children; they will ensure the above safe storage guidelines are followed at all times.

Data Checking

- The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.
- Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

Data Disclosures

- Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.
- When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.
- If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.
- Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
- Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.
- A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

Data relating to issues that involve child protection and safeguarding will adhere to the guidelines set out to the school's Child Protection Officers.

Photographs

Photographs taken purely for personal use are exempt from the Data Protection Act. This means that parents, friends and family members can take photographs for the family album of their children and friends participating in school activities and can film events at school. The Data Protection Act does apply where photographs are taken for official use by schools and colleges, such as for identity passes, and these images are stored with personal details such as names. Where the Act does apply, it will usually be enough for the photographer to ask for permission to ensure compliance with the Act. The Information Commissioner's Office has issued practical guidance on this subject.

Subject Access Requests

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

The Data Protection Act gives individuals the right to be told what 'personal data' an organisation is processing about them and, unless an exemption applies, to receive a copy of that information.

- If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.
- Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

Data management – Data Protection Policy & Procedure
Data protection law reinforces common sense rules of information handling, which most organisations try to follow anyway. It is there to ensure that organisations manage the personal information they hold in a sensible way. Organisations must keep the information accurate and up to date, they must only keep it for as long as they need it for a specified purpose and they must keep it secure.

Definition
"Data" is information that can be stored either on equipment (i.e. computer) or physically (i.e. in a filing system), or is information that forms part of an accessible record.

Bristol Steiner School Data Protection Policy
The school will comply with:

- The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.
- Information and guidance displayed on the Information Commissioner's website (www.dataprotection.gov.uk).
- This policy should be used in conjunction with the school's Internet Use Policy & the Data in Transit Policy.

Data Gathering

- All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.
- Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

Data Storage

- Personal data will be stored in a secure and safe manner.
- Electronic data will be protected by standard password and firewall systems operated by the school.
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting in the office.
- Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
- Particular attention will be paid to the need for security of sensitive personal data.
- Teachers who may need to work on children's files at home will remove any identifiable information to protect the identity of individual children; they will ensure the above safe storage guidelines are followed at all times.

Data Checking

- The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.
- Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

Data Disclosures

- Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.
- If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.
- Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
- Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.
- A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

Data relating to issues that involve child protection and safeguarding will adhere to the guidelines set out to the school's Child Protection Officers.

Photographs
Photographs taken purely for personal use are exempt from the Data Protection Act. This means that parents, friends and family members can take photographs for the family album of their children and friends participating in school activities and can film events at school. The Data Protection Act does apply where photographs are taken for official use by schools and colleges, such as for identity passes, and these images are stored with personal details such as names. Where the Act does apply, it will usually be enough for the photographer to ask for permission to ensure compliance with the Act. The Information Commissioner's Office has issued practical guidance on this subject.

Subject Access Requests
The Data Protection Act gives individuals the right to be told what 'personal data' an organisation is processing about them and, unless an exemption applies, to receive a copy of that information.

- If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.
- Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

Data in Transit Policy
Sensitive and confidential data must be treated with appropriate security by all who handle it. 'Appropriate' is not defined in terms of hard and fast rules, but is meant to be a degree of precaution and security proportionate to the potential impact of accidental disclosure. It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore staff handling sensitive and confidential data MUST assume personal responsibility and make considered judgements in terms of how they handle data whilst delivering their service.
Overall impact is determined by the degree of sensitivity of the data and the quantity involved, but we must remember that a single record about an individual can have a potentially massive impact on that individual if accidentally disclosed to others.

Key points:
- All staff are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data is protected.
- All sensitive and confidential electronic data being taken outside of its normally secure location must be password protected.
- Data loss must be reported immediately to the School Business Manager.
- Disciplinary action will be taken where staff do not follow the guidance set out in this Policy.

Purpose
This document is intended to prevent unauthorised disclosure of information by laying down clear standards of practice to maintain good security when using, taking or sending sensitive or confidential data outside of their normally secure location. This duty arises from legislation relating to information security, the most notable of which is as follows;
- Data Protection Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 2000

Scope and who the policy applies to
The scope covers all circumstances where sensitive or confidential data are taken outside of its normally secure location. This includes data in all formats – non-electronic (paper) and electronic (e.g. on PCs, tablets, laptops and removable storage media – i.e. USB memory sticks, PDAs etc.).
Whilst the Policy refers to permanent staff it also applies to temporary staff, volunteers, students and work experience candidates.

'Common Sense' Precautions
There are some 'common sense' precautions that staff and members can take before sending or taking sensitive or confidential data outside of its normally secure location, these are:
- Check that you are not sending/taking more detail than is necessary i.e. will the information still meet the need if you remove the sensitive material?
- Check that the data you are sending/taking are correct and appropriate.
- Check that you are sending the data to the correct person/address.
- Check how you intend to keep it secure.

Mobile Storage Devices
If you are taking data with you on a mobile storage device, such as a tablet PC, laptop or a USB memory stick, they must be password protected and you must:

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- Make sure that there is no other more secure option available to you
- Take only as much as necessary, for as long as necessary and transfer them back to their normally secure location as soon as possible.
- Keep the decryption password separately from the device/data
- Take all reasonable precautions to keep the device and data safe and secure e.g.:
    1. Keep it with you whenever possible; lock it away securely when you can't
    2. Never leave it in plain sight in public places
    3. Never let others use your access or device
    4. Delete the data from the device as soon as possible
    5. Report loss/theft immediately

Post

The postal service is considered reasonably secure for small amounts of low impact data (i.e. records pertaining to an individual, but NOT including very sensitive personal data – see Data Protection Act on-line training). There are precautions that you must take to prevent loss:

- Make sure that the recipient and destination address is correct, accurate and up-to-date
- Clearly mark the envelope/parcel with a return address in case of incorrect delivery
- Do not send the only copy of the data if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- If you use a courier they must be known and trusted
- Make sure it is traceable (i.e. confirmation of receipt)
- Physical records must be sent in a suitable container i.e. robust and secure enough to prevent accidental loss and/or tampering

Home PC/laptop

If you are working at home on your own PC or laptop you must:

- Only have as much sensitive or confidential information open as necessary and only for as long as necessary – do not save the data on your machine and do not leave the connection open when you are not actively working on it
- Always save the data back to their normally secure location when you have finished
- You must not leave the computer unattended for any period of time such that others can access any sensitive data; always lock the computer or log out when you are not using it, or set it to automatically revert to log-in page after a specified short period of inactivity.

Fax

Sending sensitive or confidential information by fax is a last resort and should only be used if the need is urgent and there is no alternative available and you must:

- Make sure the receiving fax machine is in a secure environment
- Make sure the recipient is there to receive it at the time of arrival and that they are known and trusted
- Make sure it is traceable (e.g. confirmation of receipt)

You must not!

There are some data handling activities which simply must be avoided:

- Sending sensitive or confidential information in unencrypted electronic form at any time.
- Sending sensitive or confidential information as unsecured physical records.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- Working on sensitive or confidential data on a public PC/laptop (for example in a library or cafe).
- Working on sensitive or confidential data on a PC or laptop with an unencrypted wireless (WiFi) connection, i.e. ensure your home wireless network has encryption and use it.
- Leaving sensitive or confidential physical records in plain view of others (i.e. on the back seat of your car, in a public place, on your kitchen table or even with you, but where they can be overlooked by others).

Physical (Paper) Records
If you are taking sensitive or confidential information with you in non-electronic (paper) records you must:

- Make sure that there is no other option available to you
- Never take the only copy with you if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- Take only as much as necessary and only for as long as necessary
- Transfer it back to its normally secure location as soon as possible
- Take all reasonable precautions to keep the records safe and secure e.g.:
    1. Keep them with you whenever possible; lock them away securely when you can't
    2. Use a suitable container that prevents accidental loss and/or viewing by others
    3. Never leave them in plain sight in public places
    4. Report loss/theft immediately

Reporting Data Loss
In the first instance staff should report a loss of sensitive and/or confidential data to the School Administrator, who will determine the significance of the loss and will take appropriate action notifying the Chair of Trustees.
The Executive Group will investigate the circumstances of the loss and will be responsible for taking corrective action to prevent re-occurrence.

Methods of data transit and storage
The following is a list of methods and devices commonly used to store and/or transfer data outside of their normally secure location.

- Email
- Fax
- Post
- Mobile devices:
    1. Laptops & tablet PCs
    2. CD/DVDs
    3. PDAs - IPAQs
    4. Smart phones - QTEK, Mobile 5
    5. Mobile Phones
    6. USB flash/hard drives - memory sticks
    7. Cameras, dictaphones
- Home PC/laptop
- Public PC/laptop (e.g. in a library or cafe)

Normally Secure Location
For the purposes of this policy standard 'normally secure location' is defined as:

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- A secure network/storage facility with:
  1. Access controls such as individual login accounts
  2. Backup and recovery facilities
  3. No public access
  4. Anti-virus and firewall protection

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

Data Management: Emailing Confidential Documents

1. **How do I decide if I can email a document?**

Most emails can be sent with names without any concerns for data protection. (E.g. Jenny forgot her wellies today).

A good Rule of thumb is: If I am happy to put a copy of that email on the Schools front door for anybody to see, then I know I don't need to worry about data protection. Otherwise, you need to be thinking of encrypting the information into an attached word document.

NOTE: Children's names should never be used in the Subject or body of an email that contains sensitive data even if the attachment is encrypted.

2. **YOU WANT TO SHARE A CONFIDENTIAL DOCUMENT/IMAGE INSIDE THE SCHOOL**

All you have to do is put that document/image in a CONFIDENTIAL folder on the network and let the other person know where it is by email. E.g. DSL/SMT should use the safeguarding folder as only people with password can access those folders.

Never give passwords out to any of our school accounts, refer them to Natasha if there are any problems.

If you find you need a secure folder as the Teachers and Staff private folders are visible to staff, please let me know.

3. **YOU WANT TO SCAN A CONFIDENTIAL DOCUMENT**

You need to use the Scan to Network not Email as follows:

- One the Printer, look for your name in the Alphabet buttons on the top. Your name should have Name & Scanner after it (e.g. Jo Scanner) DO NOT USE THE EMAIL SCANNER FUNCTION AS THIS WILL EMAIL THE DOCUMENT OUT OF OUR NETWORK.
- When the document is in the matching, press that BUTTON and then START
- Now go do your folder in 1 - Staff Private Folders on the server.
- Your document should appear in there.

4. **YOU WANT TO EMAIL A CONFIDENTIAL DOCUMENT OUTSIDE THE SCHOOL**

So you may have a document you need to send by email but you know it has to be protected because it has sensitive data. You can use Microsoft Word to create a password protected document that can be attached to an email as follows:

- Create the Word document as usual or open an existing document.
- Go to FILE and then on the right click on PROTECT DOCUMENT
- Create a password ensuring there is at least two !! (exclamation marks) a capital letter, a number and it's a minimum of 10 characters. This is vital to ensure the security of each document: EXPERT SAYS: length: 10, complexity: a-zA-Z0-9 + symbols ==> 91800 years to brute force it open.
- Word will ask you to enter the password twice.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- Then click on SAVE icon (the little floppy disc). It may ask you to save AS and all this means is you make another copy of that document with a new name and you email that document instead.
- CLOSE and REOPEN the document you are sending to be 100% sure it's encrypted.
- Phone the person you are sending the document to and give them the password. [DO NOT EMAIL THE PASSWORD PLEASE]

Data Management: Email Policy & Procedure
This policy is part of the school's data protection policy. It aims to protect any confidential data of parents and pupils that may be transmitted electronically, to ensure that staff use safe electronic procedures, and to protect the professional integrity of staff in terms of data usage and transmission.

Email accounts
All staff should acquire and use a BSS domain email address wherever practicable for communicating professional and work-related information.

Where it is not possible to use a BSS email address for professional purposes, staff must ensure they create an email account which is separate from their personal accounts.

All email accounts used for professional purposes must have a secure password. *(A secure password must have at least 8 characters and must contain a mixture of alphabetic and non-alphabetic keys. The password should not comprise whole words, even if you have substituted numbers for some of the letters.)*

It is important to remember to sign out from secure accounts.

Sending confidential information by email

Personal information, including pupils' full names, may not be sent by open email, with some exceptions for mails sent exclusively within the school's domain.

Where it is unavoidable to send some personal information by email, work from a 'need to use'
principle: e.g. if an initial is clear enough, use it rather than a full name: only repeat a name or other data in a reply if it is absolutely necessary. Do not include full names of subjects of photos in the same email.

Class lists, waiting lists and documents containing a comparable level of personal data may not by sent by email without using a secure attachment; paper copies are preferable wherever possible.

Creating a new email
Choose the subject header carefully. ***Never*** use a personal name in the header, or any wording that could draw the attention of hackers.

Never use a child's full name in the body of your message. Within the school's domain, you may use a first name and an identifier such as an initial of the surname or the class number, but best practice is not to do so, and this should not be done in mails outside of the school's domain.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

Do not use more than one piece of identifying personal data in the body of your message – for example do not give a date of birth if you have given a name. If you need to send this level of confidential information, consider the following options:

- Make a telephone call instead
- Post a letter instead
- Send a fax instead (so long as you are confident the recipient will receive the fax in person)
- Use an electronic storage device (but only if it has a secure password and the data is encrypted)
- Send the information in a secure attachment (see below)
- Admin staff should consider using the Department for Education's s2s encrypted website

When sending out application forms for pupil admissions or staff vacancies, the applicants should be advised to return their completed form by post, fax or by a secure password protected attachment.

Before clicking the send button:

- Slow down – it is very easy to make an error in haste
- Read through your response and consider whether your wording could be misinterpreted in any way – any email you send could be considered an official response from the school, and should be worded accordingly
- Check the 'TO:' line (i.e. the recipient's name/address). Most email software fills in addresses automatically – check it has done so correctly.

Replying to and forwarding emails

- Scroll down to check the sender's original message(s). If there is any personal data contained in it, either delete their message entirely or amend it to avoid re-sending the personal information. Just because someone else has sent sensitive data does not justify you doing the same.
- Check the sender's name/address – be sure you are sending it to the right person and not a group (unless that is what you intend)

Sending emails to more than one person

If you wish to mail several people, it is good practice to send your mail as a blind carbon copy (BCC) so as not to reveal private email addresses. This also applies when you send out a mail to a group you may have created (unless there is a mutual agreement, for example a class email group).

Secure Attachments

Attachments may only be used to send confidential information if they are both encrypted and protected with a secure password. Agree the password with the recipient, ideally by telephone, but otherwise in a separate email.

To protect the content of attachments, consider making the document read only.

Storing emails

An email inbox is not a safe form of storage. Do not store emails containing sensitive data. If such data is in the body of the mail, preferably cut and paste it into a Word document and

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

save the file with your documents, then delete the email, otherwise delete the relevant data or print and file a paper copy if necessary.

On receipt of an attachment containing personal data, again, either print it out or save it to your documents and delete the email immediately.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

Data Management: Photography Policy

Photography is subject to the Data Protection Act 1998 regarding the rights of individuals to have information of a personal nature treated in an appropriate manner, and the Human Rights Act 1998, protecting the privacy of individuals and families. As well as these statutory rights, restrictions on photography arise from issues of child protection and copyright of performance.

Photographs and video for school and family use are a source of innocent pleasure and pride, which can enhance the self-esteem of children and young people and their families. Parents are not required to comply with the Data Protection Act 1998 when taking photographs for their own private use of their children at an organised event. Parents should not be stopped from taking photographs for their own private use because of concerns of contravening the Data Protection Act. However we must always be mindful of the need to safeguard the welfare of children in our school, and issues of child protection, data protection and parental consent will be given careful thought. Images may be used to harm children, for example as a preliminary to 'grooming' or by displaying them inappropriately on the Internet. This policy will apply to all forms of publications; print, film, video, DVD, on websites, social media (Facebook etc.), and in the professional media as well as images recorded on mobile phones.

Aim

BSS aims to comply with the law and to protect and respect the privacy of the children and their families and all other members of the school community. For this reason we require the consent of either the individual concerned or in the case of pupils, their legal guardians before we can display images in the media, in publications, on websites or in public places.

Safeguarding Issues

Risk occurs when individual pupils can be identified by their names alongside photographs. Therefore we will only name the children in photographs that are displayed within classrooms. We will not provide names for any other purpose unless special parental consent has been received. Also, the content of the photograph can be used or adapted for inappropriate use. Therefore only images of children in suitable dress will be taken. Should the School learn about any inappropriateness of image use involving our pupils, we will immediately act and report it as we would for any other Safeguarding issue.

Use of images

Parents

- The School will decide if the event is one at which photography and videoing will be permitted.
- When informing parents of the event, they will be informed of the School's decision
- If general photos are to take place at public events such as at a School fair, visitors will be warned in the publicity & invitations, so that general consent is implied by attendance. This will be announced in the programme for these events.
- Only images of children suitably dressed will be allowed to reduce the risk of images being used inappropriately. Special consideration will be given to photographs taken during PE (sports day) and swimming.

School

- If a photograph is likely to be used again it will be stored securely and only accessed by those people authorised to do so.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

- Digital copies of images will be stored securely on school computers with password protected servers.

Images taken by Children

- The use of cameras within school (when requested and authorised), on trips or visits is part of the pleasure and the learning in the experience.
- There is no reason why pupils should not be allowed to take photographs so long as anyone photographing respects the privacy of the person being photographed.
- Infringement of this respect of privacy is akin to bullying and will be dealt with in the same way as any other breach of school discipline.

Guidance for parents

- Written guidance will be given to parents to the effect that any images must be taken for personal use only and specify that images including others must not be put on the web/internet, and that if they are Data Protection legislation may be contravened. Information will be sent via the school website and newsletter, and reminders will be given by teachers at the start of school festivals, plays etc.
- A copy of the 'Use your camera and video courteously' code' will be given to all parents.
- Parents will be prompted with a verbal announcement at the start of any events, plays, celebrations of work etc. whether photography/recording is permitted.
- If permitted parents will be reminded that any images must be taken for personal use only and that such images must not be sold or be put on the web/internet/social media otherwise Data Protection legislation is likely to be contravened.
- People with no connection to our School will not be allowed to photograph children– staff will question anyone they do not recognise who is using a camera and or video recorder at events and productions.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

‘**Use your camera and video courteously’**

A guide for parents who wish to use photography and/or video a school event

Generally photographs and videos for school and family use are a source of innocent pleasure and pride, which can make children, young people and their families feel good - about themselves. By following some simple guidelines we can proceed safely and with regard to the law.

- The Headteacher has the responsibility to decide if photography and videoing of School performances is permitted and also to decide the conditions that will apply so that children are kept safe and that the performance is not disrupted and children and staff not distracted.

- When permitted -parents and carers can use photographs and videos taken at a School event for their own personal use only. Such photos and videos must not be sold and must not be put on the web/internet (including social media). To do so may breach Data Protection legislation.

- Recording or/photographing other than for your own private use would require the consent of all the other parents whose children may be included in the images.

- Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity.

- Parents and carers must not photograph or video children changing for performances or events.

- If you are accompanied or represented by people that School staff do not recognise they may need to check who they are, if they are using a camera or video recorder.

- Remember that for images taken on mobiles phones the same rules apply as for other photography, you should recognise that any pictures taken are for personal use only.

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257

ICT Parent Consent Form and Pupil Declaration

Please complete and return to the office

Pupil's name ……..

Pupil declaration:
As a user of the school's ICT facilities, which includes the internet I have read the school's ICT Code of Conduct and I agree to comply with all the points contained therein. I will use the facilities, including the internet, responsibly and I will observe all the restrictions imposed by the school. I understand that any breach of the Code of Conduct may result in withdrawal or restriction of my access to the School's ICT facilities.

Pupil Signature …….

Date …….. / …….. / ……..

Parent/Guardian consent:

As Parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the ICT facilities at school, which includes the internet. I understand that pupils will be held accountable for their own actions. I also understand that some *materials* on the internet may be objectionable and I accept my part in being responsible for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media.

Parent / Guardian Signature ……

Date …… / ……. / ……

Bristol Steiner School, Redland Hill House, Redland Hill, Redland, Bristol. BS6 6UX
Telephone: 0117 933 9990 Facsimile: 0117 933 9999
E-mail: reception@bristolsteinerschool.org Website: www.bristolsteinerschool.org
Member of the Steiner Waldorf Schools Fellowship Company Number 1131462 Charity Number 310257