Salterford House
Preparatory School

E-Safety Policy

This policy has regard for Part 3 The Education (Independent School Standards) Regulation 2014, in force January 2015.

It is a whole school policy, including EYFS, and should to be read in conjunction with:

Keeping Children Safe In Education 2016

The school's: -

Safeguarding and Child Protection Policy

Recruitment Policy

Prevent Policy

Staff Code of Conduct

It includes:

- The Agreement for e- Safety rules for children
- Parent e- Safety Acceptable Use Agreement
- e- Safety Acceptable Use Agreement/ Code of Conduct for Staff and Visitors
- Image Consent Form
- e- Safety Risk Assessment

1 Introduction

Computing and other technologies in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently schools need to build in the use of these technologies in order to arm children and young people with the skills to access life-long learning and employment.

Computing and other technologies 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 IT within our Society as a whole. Currently, the internet technologies children and young people are using both inside and outside the classroom include:-

- Apps
-
- E-mail, Instant Messaging and Chat Rooms
-
- Social Media, including Instagram
-
- Mobile/Smart phones with text, video and/or web functionality

-
- Other mobile devices, including tablets and gaming devices
-
- On-line games
-
- Learning Platforms and Virtual Leaning Environments
-
- Blogs and Wikis
-
- Podcasting
-
- Video Sharing
-
- Downloading
-
- On Demand TV and video, movies, radio and Smart TVs

Whilst exciting and beneficial both in and out of the context of education much IT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

We understand the responsibility to educate our children on eSafety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, both in and outside the classroom.

We hold personal data on our children, staff members, parents and others to help conduct day to day activities. Some of this information is sensitive and could be used by another person to cause harm or distress to an individual. The loss of sensitive information can result in media coverage and potentially damage the reputation of the school.

We all have a shared responsibility to secure any sensitive information used in day to day professional duties and we understand that our staff, even though they may not be directly involved in data handling, will be made aware of risks and threats that may occur and how to minimise them.

Both this Policy and the Acceptable Use Agreement (for staff members, regular visitors and children) are inclusive of both fixed and mobile Internet technologies provided by the school (such as laptops, PCs, mobile devices, webcams, whiteboards, digital video equipment etc.) and technologies owned by the children and staff, but brought into school (such as laptops, mobile or smart phones, Ipads and other mobile devices).

2. **Monitoring**

The Head Teacher and her Deputy may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, Internet/Intranet use and any other electronic communications (data, voice, video or image) involving its employees, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information, to confirm or investigate compliance with school policies, standards and procedures, to ensure the effective operation of the school IT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

All monitoring, surveillance or investigative activities comply with the ***Data ProtectionAct 1998***, the ***Human Rights Act 1998***, the ***Regulation of InvestigatoryPowers Act2000 (RIPA****)* and the ***Lawful Business Practice Regulations 2000***.

It is important to note that personal communications using school IT may be unavoidably included in any business communications that are monitored.

3. **Breaches**

A breach or suspected breach of policy by a school employee, contractor or child may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action, in accordance with the school's Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6th April 2010, allowing the Information Commissioner's Office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the ***Data Protection Act***.

The data protection powers of the Information Commissioner's Office are to:-

- conduct assessments to check organisations are complying with the Act
-
- serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period
-
- serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law
-
- prosecute those who commit criminal offences under the Act
-
- conduct audits to assess whether organisations' processing of personal data follows good practice
-
- report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head Teacher or her Deputy. Additionally, all security breaches, lost or stolen equipment or data (including remote access), virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be reported to the Head Teacher, her Deputy or the eSafety Co-ordinator.

4. **Acceptable Use**

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both inside and outside school and to be aware of their responsibilities towards their children. We regularly consult and discuss eSafety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with possible associated risks.

Parents/carers are asked to read through and sign Acceptable Use Agreements for eSafety on behalf of their child on admission and annually thereafter until the child leaves.

All children use computer facilities, including Internet access, as an essential part of learning. Both children and their parents/carers are asked to sign, to show that the School eSafety Rules have been understood and agreed.

5. **School ICT Equipment, including Portable and Mobile IT Equipment and Removable Media**

School IT Equipment:
As a user of school IT equipment you will be responsible for your activity

•Ensure that all IT equipment that you use is kept physically secure.

•Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

•Personal or sensitive data should not be stored on the local drives of a desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so, the local drive must be encrypted.

•It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.

•Privately owned IT equipment should only be used on the school network with the express permission of the Head Teacher or eSafety Co-Ordinator.

•It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

•All IT equipment allocated to staff must be authorised by the Head Teacher or the eSafety Co-Ordinator.

•All redundant IT equipment must be disposed of in accordance with Waste Electrical Equipment (WEEE) directive and the Data Protection Act (DPA).

Personal Mobile Devices:

•The school allows staff members to bring in personal mobile phones and devices for their own use. Contacting a child or parent/carer using a personal device is only permitted in an emergency with permission from the Head Teacher.

•Children are not allowed,to bring personal mobile phones and devices into school.

•The school is not responsible for loss, damage or theft of any personal mobile phone or device brought into school.

•Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

•Users bringing personal mobile telephones or devices into school must ensure that there is no illegal content on the device.

•

School Provided Mobile Devices:

Where the school provides mobile technologies, such as laptops or Ipads for off-site visits and trips, only these devices should be used on such occasions.

6. **Computer Viruses**

•There should be no interference with anti-virus software installed on school IT equipment.

•Personal equipment used in school, which is not part of the school's hardware must be subject to regular virus updates; unprotected equipment should never be brought into school.

•If a virus is suspected on any school IT equipment, its use must be stopped and the Head Teacher and/or eSafety Co-Ordinator informed without delay.

7. **Data Security**

•The school gives relevant staff members remote access to files with a unique username and password.

•It is the responsibility of all staff members to keep passwords secure.

•Staff members are aware of their responsibility when accessing school data.

•Staff members have been issued with the relevant guidance documents and the Policy for eSafety Acceptable Use, including information in their Staff Handbook.

•Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.

•Staff members should avoid leaving any portable or mobile IT equipment or removable storage media in unattended vehicles.

•Staff members should always carry portable and mobile IT equipment or removable media as hand luggage and under their control at all times.

•It is the responsibility of individual staff members to ensure the security of personal, sensitive, confidential and classified information, which is contained in documents, copied, scanned or printed.

Sensitive Information

Any information that is sensitive must be protected. This will include personal data of children and staff members, such as assessment records, medical information and special educational needs data. The Head Teacher will:-

•decide what information is held and for what purposes

•decide what information needs to be protected, how information will be amended or added to over time

•decide who has access to data and the reason

•decide how information is retained and for how long and the method for its eventual disposal

However, it should be clear to all staff members that the handling of secured data is everyone's responsibility, whether they are an employee, a volunteer or a managed service provider. Failure to apply appropriate controls to secure data may amount to gross misconduct or even legal action.

<u>Remote Access</u>

•All staff members are responsible for all activity via their remote access facility.

•Staff members will ensure that they only use equipment with an appropriate level of security for remote access.

•Staff members should avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

•Staff members must protect school information and data at all times, including any printed material produced whilst using the remote access facility. Particular care should be taken when access is from an environment outside school.

8. Disposal of Redundant IT Equipment Procedure

All redundant IT equipment will be disposed, with all data removed, or if the storage media has failed it will be physically destroyed.
Disposal of any IT equipment will conform to:-

•The Waste Electrical and Electronic Equipment Regulations 2006

•The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

•Data Protection Act 1998

9. **Email**

The use of email is an essential means of communication. In context of school, email should not be considered private. Educationally, email can offer significant benefits, including direct written contact between schools on different projects, be they staff or children based, within the school or international. We recognise that the children need to understand how to style an email in relation to their age and how to behave responsibility on-line.

Managing Email

•The school gasks all staff members to use the office email account to use for all school business as a work based tool. This is to protect them, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

•Staff members should use the school email for all professional email communication.

•Under no circumstances should staff members contact the children, parents/carers or conduct any school business using their personal email address.

•All emails should be written and checked carefully before sending, in the same as a letter written on school headed letter paper.

•Staff sending emails to external organisations, parents/carers or children are strongly advised to cc: the Head Teacher.

•Children may only use school approved accounts on the school system for education purposes and then only under direct teacher supervision.

•All child email users are expected to adhere to the generally accepted rules of responsible on-line behaviour, particularly in relation to the use of appropriate language, and not reveal any personal details about themselves or others in email communications, or to arrange to meet anyone.

•Children must immediately tell a teacher or trusted adult if they receive an offensive or upsetting email.

•Staff must inform the Head Teacher or eSafety Co-Ordinator it they receive an upsetting or offensive email.

•Children are introduced to email as part of the Computing Programme of Study.

•However a school email account is accessed (whether directly through webmail when away from the office or on non-school hardware) all the school policies must be adhered to and still apply.

Receiving Emails

•School email accounts must be checked regularly by the office manager.

•Attachments from an unknown or untrustworthy source must never be opened.

•All unsolicited emails should be deleted from the school email account.

•

10. Equal Opportunities

Children with additional needs

Staff members are aware that some children may require additional support or teaching, including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a child has a poor social understanding, careful consideration must always be given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for such children.

11. eSafety
eSafety – Roles and responsibilities

ICT and on-line resources are increasingly used across the curriculum. We believe that it is essential for eSafety guidance to be given to children on a regular and meaningful basis, which is easily understood. eSafety is embedded in our Curriculum and we continually look for new opportunities to promote eSafety.

•The school has a framework for teaching Internet skills in Computing and PHSEE lessons

•The school provides opportunities, within a range of Curriculum areas, to teach about eSafety.

•Educating children about on-line risks that they may encounter outside school is done informally, when opportunities arise and as part of eSafety guidance and PHSEE.

•Children are taught about Copyright, respecting other peoples' information, safe use of images and other important areas through discussion, modelling and appropriate activities.

•Children are aware of the impact of Cyberbullying and know how to seek help if they become the subject of any form of on-line bullying. Children are also aware of where to seek advice of help if they experience problems using the Internet and related technologies, ie: parent/carer, teacher/trusted staff member, Childline or CEOP Report Abuse Button.

E-Safety skills development for staff members

•Our staff members receive regular information and training on eSafety and how they can promote 'Stay Safe' on-line messages.

•New staff members receive information on the school's eSafety Acceptable Use Policy as part of their induction programme.

•All staff members have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.

•All staff members are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up to date areas of concern.

Managing the school eSafety messages

•We endeavour to embed eSafety messages across the Curriculum, whenever the Internet and/or related technologies are used.

•The eSafety Policy is introduced to the children at the start of each Academic Year.

•The key eSafety advice will be promoted widely, throughout the school displays, newsletters, classroom activities etc.

12. Incident Reporting, eSafety Incident Log and Infringements

Incident reporting

All security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be recorded and reported to the Head Teacher or eSafety Co-Ordinator. The eSafety Incident Log is held in the main office and will be monitored termly by the eSafety Co-ordinator and all incidents discussed with the Head Teacher.

13. Internet Access

The Internet is an open, World-wide communication medium which is available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education and business, a forum for social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

•The school provides children with supervised access to Internet resources, through the school's fixed and mobile Internet connectivity.

•Staff members will review any recommended sites, on-line services and apps before they are used.

•If Internet research is set for homework, specific sites will be suggested that have been previously checked by the Teacher. It is, however, strongly advised that parents re-check these sites and supervise this type of work. Parents will always be asked to supervise further work.

•All users must observe Copyright at all times.

Managing other on-line technologies

On-line technologies (including social network sites), if used responsibly, both outside and within an educational context can provide easy to use, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our parents/carers and staff members to think carefully about the way information can be added and removed by all users, including themselves, from these sites.

•At present, we endeavour to deny access to social networking to all children within school.

•Specific online educational sites are used in school and at home, but logins and passwords are given monitored.

•All children are advised to be cautious about the information given by others on such websites, eg: users not being who they say they are.

•Children are taught to avoid placing images of themselves (or details within images that could give background details) such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once it is on-line.

•Children are always reminded to avoid giving out personal details on websites, which may identify them or where they are (full name, address, mobile/home phone number, school details, email addresses, specific hobbies/interests etc.)

•Our children are advised to set and maintain their own on-line profiles to maximum privacy and deny access to unknown individuals.

•Children are encouraged to be wary about publishing specific and detailed private thoughts and information on-line.

•Our children are asked to report any incidents of Cyberbullying to the school

•Services such as Facebook and Instagram have a 13+ age rating, which should not be ignored.

14. Passwords and password security

Zombie Accounts
Zombie accounts refers to accounts belonging to users who have left the school and, therefore, who no longer have authorised access to the school's systems. Such Zombie accounts, when left active, may cause a security threat by allowing unauthorised access. Therefore, the school will:-

•ensure that all user accounts are disabled once a member of the school has left

•take prompt action on disabling accounts to prevent unauthorised access

•regularly change generic passwords to avoid unauthorised access

15. Personal or sensitive information

Protecting personal, sensitive, confidential or classified information
Staff members must:-

•ensure the accuracy of any personal, sensitive, confidential and classified information that they disclose or share with other people

•ensure that any such information is not disclosed to any unauthorised person

•ensure the security of any such information that they copy, scan or print. This is particularly important when shared printers (multi-function, print, scan and copiers) are used and when access is from a non-school environment

•only download personal data from systems if they are expressly authorised to do so by the Head Teacher

•Keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information

•

16. Safe use of images

Taking of images and film

Digital images are easy to capture, reproduce and publish and, thus, misuse. Everyone must remember it is not always appropriate to take or store images of a member of the school community or a member of the public without first seeking consent and considering the appropriateness of such an action.
With the written consent of parents/carers (on behalf of all children) and staff members, the school permits the appropriate taking of images by staff members and children using school equipment.

Staff are not permitted to use personal digital equipment, such as smart and mobile phones or cameras to record images of children and other members of the school community and this includes when on field trips, unless they have the express permission of the Head Teacher and the images are transferred as quickly as possible and solely to the school's network. The images must then be deleted immediately after transfer from the staff member's device.

Children and staff members must have permission from the Head Teacher or Lead Designated Person for Safeguarding before any image may be uploaded.

17. Social Media Policy

The school acknowledges that social media has become a regular part of everyday life and that many people enjoy blogs, media sharing services, social networking sites and forums and holding membership of sites such as Facebook, MySpace or Twitter.

It is very important to note, however, that the use of social media and networking websites has implications for:-

1. our duty to safeguard children;

2. your reputation and that of the school;

3. data protection;

4. confidentiality; and

5.our relationship with pupils parents, each other and the wider community.

This policy is intended to give you clear guidelines as to what the school expects from you and to help you make appropriate decisions about the use of social media to ensure that students are kept safe, that the school is not exposed to legal risk, and that the reputation of the school is not adversely affected.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and the School. It may also cause embarrassment to us and to our students and parents and so you must only use social media with caution.

We have set out various standards below which we will expect you to observe. It is incumbent upon all of us to ensure the proper implementation of this policy to protect the school each other and our pupils.

1.This policy should be read in conjunction with the:-

·Acceptable Internet Use Statement

· Staff Code of Conduct for CT

2.General

2.1. All members of the school are expected to comply with this policy at all times to protect the privacy, confidentiality and interests of the school, our staff, partners, parents and pupils.

2.2. Breach of this policy will be dealt with under the Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

3.Professional Use of Social Media

3.1. Only staff with permission are permitted to post material on a social media websites or other on-line forums in the school's name or on behalf of the school. Any breach of this restriction will amount to gross misconduct

4.Your personal use of Social Media

You are personally responsible for content you publish into social media tools; be aware that what you publish will be public for many years.

4.1.You will not:-

4.1.1 use social media during school hours

4.1.2. access social media on any school CT equipment at any time, whether during school hours or otherwise

4.1.3. upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.

4.1.4. upload, post or forward any content belonging to a third party unless you have that third party's consent

4.1.5. discuss colleagues, students, the school, other schools or suppliers without their prior approval and the approval of the Head Teacher

4.2. Your use of social media must not

4.2.1. breach the school's misconduct, equal opportunities or bullying and harassment policies.

4.2.2. be used to discuss or advise any matters relating to school, staff pupils or parents.

4.3. You must:-

4.3.1. be mindful of the impact your contribution might make to people's perceptions of you and the school.

4.3.2. always consider others' privacy and avoid discussing topics that may be inflammatory;

4.3.3. avoid publishing your contact details where they can be accessed and used widely by people you did no intend to see them

4.3.4. ensure that personal blogs have clear disclaimers that the views expressed by the author are yours alone and do not represent the views of any third party.

4.3.5. ensure any information you publish on the Internet complies with the school's equal opportunities, confidentiality and data protection policies.

4.4. If you feel slightly uneasy about something you are about to publish, then you shouldn't do it. If in doubt, always discuss it with The Head Teacher.

5.Contact with Pupils

5.1 You will not establish or seek to establish social contact via social media or other form of information communication technologies with pupils.

5.2. You will not have a pupil or former pupil under the age of 18 as a 'friend' to share information with.

5.3. You will not interact with any pupil or former pupil (under the age of 18) on social networking sites.

Should a pupil attempt to join your area on a social networking site you must inform the Head Teachers. Parents will be informed if this happens.

6.Personal Data

6.1. Never disclose sensitive, private or confidential information regarding, the school including but not limited to any student, parent or member of staff.

6.2. Make sure that others cannot access any content, media or information from your profile that would undermine your position as a professional, trusted and responsible person.

6.3. You should consider:-

6.3.1. reviewing the privacy settings on your profile so that only people you have accepted as friends can see your content

6.3.2. regularly reviewing who is on your 'friends list' on your personal profile

7.Notify

7.1. Breaches of this policy should be notified to the Head Teacher and action will be taken in respect of any such breaches.

7.2. Any member of staff who feels that have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the Head Teacher.

7.3. The terms and conditions of most social media and networking sites do not allow members under the age of 13. If you become aware of any of the pupils using or accessing social media sites then please inform the Head Teacher immediately.

7.4. If you notice any content posted on social media about us (whether complimentary or critical) please report it to the Head Teacher.

8.Evidence of Misuse:-

8.1. Where evidence of misuse is suggested we will undertake a more detailed investigation in accordance with our Disciplinary Procedure.

8.2. If necessary such information may be handed to the police or other bodies including but limited to LADO

Remember, at all times, in or out of working hours, in social media or otherwise, you are an ambassador for the school.

9. Writing and reviewing this policy

Review Procedure
There will be on-going opportunities for staff to discuss with the e-Safety Co-Ordinator any e-Safety issue that concerns them.
This policy will be reviewed annually and consideration will be given to the implications for future whole school development planning.
The policy will be amended if new technologies are adopted.

Acceptable Use

Agreement of e-Safety Rules – KS2 Children

I will only use IT in school for school purposes

I will only open/delete my own files

I will make sure all IT contact with other children and adults is responsible, polite and sensible

I will not look for, save or send anything that could be unpleasant or nasty. If I accidently find something like this I will tell my teacher immediately

I will tell my teacher immediately if I see anything on-line which makes me feel uncomfortable

I will not give out my own or others details, such as name, phone number or home address.

I will not arrange to meet or send an image unless this is part of a school project approved by my teacher

I will be responsible for my behaviour when using IT and understand that these rules are to keep me safe

I will support the school approach to on-line safety and not upload or add any images, video, sounds or text that could upset any member of the school community

I know that my use of IT can be checked and my parent/carer contacted of a member of school staff is concerned about my safety

I will not sign up for any on-line services, unless this is an agreed part of a school project approved by my teacher and I am old enough to do so

I will not bring a Smart Watch to school, because I am not allowed to wear one in school
These rules help me to stay safe on the Internet
Think then Click

eSafety Rules for Early Years and KS1 Children

We always ask an adult if we can use the Internet

We may click on the buttons and links only when we know what they do

We only use apps and websites that an adult has chosen

We tell an adult if we see anything that makes us feel uncomfortable

We never give out information about ourselves or passwords

We do not use Internet Chat Rooms

Parent e-Safety Acceptable Use Agreement

IT, including the Internet, email and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using IT.

Please read and discuss these eSafety rules with your child(ren) and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact Mr M Britten.

Please take care to ensure that appropriate measures are in place at home to protect and support your child(ren) on-line.

………………………………………………………………………………

- I have read and understood the school's eSafety Acceptable Use Agreement and give permission for my child to access the Internet in school
-
- I understand that Internet use by my child(ren) will be supervised by an adult
-
- I understand that the school will take all reasonable precautions to ensure that my child cannot access inappropriate material
-
- I will sign the consent form held in school for my child(ren) upon their entry into school and annually thereafter

Signed:……………………………………………………

Name:……………………………………………………...

Child's Name:………………………………………………..

Staff and Visitors Acceptable Use Policy

IT (including data) and the related technologies, such as email, the Internet and mobile devices are an expected part of our daily working lives at school.

This Agreement/Code of Conduct is designed to ensure that all staff members are aware of their professional responsibilities when using any form of IT. All staff members are expected to sign this agreement and adhere to its contents at all times.

Any concerns or clarification should be discussed with the Head Teacher or eSafety Co-Ordinator.

- I will only use the school's Internet, Intranet and any related technologies for professional purposes or for uses deemed acceptable by the Head Teacher or the eSafety Co-ordinator.

- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff members are compatible with my professional role.

- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account or any other social media link to pupils.

- I will only use the approved, secure email system for any school business.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely with the express permission of the Head Teacher or her Deputy.

- Personal or sensitive date taken off site must be encrypted, eg: on a password secured laptop or memory stick.
-
- I will not install any hardware or software without the express permission of the Head Teacher or the eSafety Co-Ordinator.

- I will not browse, download, upload or distribute any material which could be deemed offensive, illegal or discriminatory.

- Images of pupils and staff members will only be taken and stored for professional purposes, in line with School Policy and written consent of the parent/carer or staff member.

- Images will not be distributed outside the school network without the permission of the parent/carer, staff member, Head Teacher or eSafety Co-Ordinator.
    -
- I will support the school approach to on-line safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community.
-
- I understand that all my use of the Internet and other related technologies may be monitored and logged and can be made available, upon request, to the Head Teacher.

- I will respect Copyright and intellectual property rights.

- I will ensure that my on-line activity, both in and outside school will not bring the school, my professional reputation or that of others into disrepute.

- I will support and promote the school's eSafety and Data Security Policies and help pupils to be safe and responsible in their use of IT and related technologies.

- I understand this Agreement forms part of my Terms and Conditions set out in my Contract of Employment.

User Signature:

I agree to follow this eSafety Acceptable Use Agreement/Code of Conduct and to support the safe and secure use of IT throughout the school.

Signature:…………………………………………

Date:…………………………………………..

Full Name (please print):……………………………………………………

Job Title:………………………………………………………………………….

Image Consent Form

We believe that the responsible use of images of children can make a valuable contribution to the life of the school and, in today's world where photography and film are an integral part of day to day life, our policy needs to harness the benefits whilst protecting the children. Therefore, our policies and procedures must be robust to protect the interests of the children and our staff. All procedures take account of Keeping Safe in Education (KSIE)2015 and the Data Protection Act 1998.

We take photographs of the children at school, during school field trips and during other activities that are carried on off-site. We may use these images in our School Prospectus or in other printed publications that we produce and in displays or on our website. We may also take video or webcam recordings, which may be used on our website or shared with other parents, eg: school performance.

On occasions we send images to news media, or our school may be visited by the media who will take their own photographs or film footage,, ie: of a visiting dignitary and our children may appear in these images. The news media may use the images in printed publications, on televised news programmes or on their website or other related social media channels. The media are bound by the Data Protection Act 1998. When we submit images and information to the media, we have no control over when or where they will be used. On such occasions, we may give names and ages of the children.

It is usual that parents/carers and family members take images of their child during school functions and these may well also contain images of other children. Where images contain children other than your own these images must not be used on any form of Social Media.

To comply with the Data Protection Action 1998, we need your permission before we can use images of your child.

Conditions of use:-

1 This form is valid for the period of time your child attends Salterford House School. Please write to us if you wish to withdraw consent at any time.

2 The images we take will be of activities that show the school and the children in a positive light.

3 Embarrassing or distressing images will not be used.

4 We may use group or class photographs or footage.

5 We will only use images of children that the Head or Designated Persons for Safeguarding Children deem appropriate.

6 No image would be used which would be considered to put a child 'at risk'.

7 We will make every effort to ensure that we do not allow images to be taken of children for whom we do not have permission.

8 We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However, we cannot guarantee

this and take no responsibility for the way images are used by other websites or publishers.
To give your consent to images being used in print and electronic form, please complete the information below and return the form to school.

I give permission for my child's image to be taken and used in publicity material for the school, including printed and electronic publications, video, on the website and that they can be used by the media.

Yes/No*

*Please delete as appropriate

I understand the need to act responsibly when using images that include children outside my own family.

I have read and understood the information overleaf.

Where applicable, please ensure that BOTH parents sign below.
Name of child: ____

Parent 1 Signature: ____________________________________

Parent 2 Signature: ___________________________________

Storage of images

Images/films of children are stored on the school's network.

Rights of access to this material are restricted to the teaching staff and children within the confines of the school network or other school resource.