Parkfield Community School

Pastoral Care Policy Statement/Provision

Rights of the Child:

A12: *Every child has the right to say what they think in all matters affecting them, and to have their views taken seriously.*

A27: *Every child has the right to a standard of living that is good enough to meet their physical, social and mental needs.*

A29*: Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures and the environment.* A model of emotional support at Parkfield Community School.

Research shows that children with emotional difficulties express their distress, anger and sadness in their behaviour and this often prevents them from learning. We believe that all behaviour is communication.

At Parkfield Community School all staff are committed to finding ways of supporting children who bring their emotions to school. The Pastoral Care Team in conjunction with class teachers, year group leaders and leadership help children to recognise, understand and meet positively their emotions and the emotions of others.

Why?

Making a difference.

'An investment in one child is an investment in all children' – Psychotherapist - Listening Matters.

Here at Parkfield we believe that enabling children to have healthy relationships will allow them to make the most of all learning opportunities on offer and moreover allow those children working alongside them the same opportunities.

How? – The Classroom

We recognise the vital part that the classroom environment and its teachers play in promoting all children's emotional well-being. The Pastoral Care Team (PCT) supports teachers to provide a nurturing environment whereby they can promote an optimal learning environment so that all children can become actively engaged. Teachers are encouraged to value the importance of relationship in all the work they do. Children who are in classrooms experiencing nurturing curriculum facilitated by a key adult (their teacher) will develop a better sense of awareness of their own needs, views and feelings, and as a result will become sensitive to the needs, views and feelings of others around them.

'Meet and Greet' is used with key children in order to give them a positive start to the day in a smaller group or a 1:1 and to encourage them in reaching their current targets.

We provide the 'Green Card System' which addresses children's behaviour choices in the classroom. This allows children the opportunity to think and discuss their choices, take responsibility and seek to discover alternative ways of behaving positively. This dialogue with a 'significant other' will form building blocks for the child's capacity to self-regulate.

The SEAL Room and the Rainbow Room

From its base in the SEAL Room and the Rainbow Room the PCT offers a variety of strategies to support children.

Therapeutic Interventions

We know that children benefit from being with an adult who actively listens to them while supporting them in an engaging activity. We have an Art Therapist visiting weekly that works with key children on a 1:1 and in small groups. Their role is to listen to the child and to offer creative ways of enabling children to express themselves through painting, modelling and other art activities.

1:1 Support

The PCT offers mentoring support to key children working closely alongside the class teacher both inside the classroom and out. The PCLs will set up an IBP, set targets with the child, set up a half termly action plan and then review the progress made by the child, the teacher and parents. Individual children's actions are plotted on a integration map which is regularly updated.

Nurturing

Some members of the PCT are trained in delivering 'Happy to Be Me', which is a programme that targets children with low self-esteem. In these sessions staff act as positive role models and tasks and expectations are developmentally matched. Children are assessed on entry and re-assessed so that progress can be measured.

Our Learning Mentors also support key children in developing their emotional literacy through the use of the Southampton Scaling resource.

Wider Well-Being – Whole School

Circle time in each classroom is held regularly to support children's well-being and self-esteem.

A school council allows children at Parkfield Community School the opportunity to share and put forward their ideas and thoughts about their school.

Positive relationships are fostered between pupils and lunchtime supervisors and a member of the PCT supports lunchtime supervisors with children making wrong choices to resolve conflict. Sports coaches and City Year Mentors are also used to promote positive play and interaction. We also have children that take on the role of 'playground buddies' in order to support children that may find it difficult mixing with others at playtime.

For children that find lunch time and playtime a more challenging part of the day, the SEAL room and the Rainbow Room offer a safe space for them to talk through their difficulties, reflect on their choices and discuss ways in which they can manage these times well.

Part of the integration work of the PCT is to respond to children's needs as they arise and be a listening ear in order to provide emotional support. Cultural identity and appreciation of diversity is promoted through our Rights Respecting approach and our emotional literacy learning, and is actively reinforced by members of staff on the playground.

BESD Provision

Within the Provision we are able to support children who have a higher level of social, emotional and behavioural needs. They are supported by trained staff with expertise in this area and are given regular access to 1:1 reviews, circle time and emotional literacy sessions while they are in the provision. As they move on to integrate into the mainstream setting both children and staff have a wide range of support from the PCT. We work hard at Parkfield to ensure every child has a sense of belonging and feeling safe.

Parents
The PCT is continually seeking ways to help parents who seek support with their children's social, emotional or behavioural needs. We offer parents the opportunity to meet with the PCL who will take seriously the concerns of a parent, listen and give them quality time. Parents are regularly kept informed of their children's behaviour on the green card system and at lunchtime.
The PCT seeks to help parents to feel welcome valued and supported. We have a parent link worker who supports targeted families.

At Parkfield we use the Malachi Family Support Trust to offer further help to vulnerable families. This involves working closely with parents and/or other key adults to support them in a variety of areas, and where appropriate working with the child on a 1:1.

Parkfield Community School is committed to setting up systems and policies which genuinely support inclusion. We are committed to meeting individual needs which in turn benefit all pupils at our school.

Staff
At Parkfield the well-being of our staff is extremely important. Staff are supported daily by their year group leader and the AHT for that year group. The PCL are also available to provide a listening and supportive ear.
At Parkfield we also using the Warner interview technique in order to support safe recruitment. This process can also identify areas where new members of staff may need support during their induction period which is then offered by PCL and any other appropriate member of staff.

Lynette Stables
Assistant Head, Pastoral Care
May 2016

Parkfield Community School
Lunchbox Policy

Aim of the Policy

To encourage healthy choices for all children in the school by ensuring that all food and drinks brought from home, consumed at school or on school trips provide pupils with healthy and nutritious food that is similar to food served at Parkfield School. We aim to educate our children with the skills, knowledge and understanding to enable them to make informed healthy lifestyle choices. To do that effectively we need to work in partnership with parents in securing the best for every child. There is a nationally recognised issue with obesity in the adult and child population. As a recognised National Healthy School we are committed to ensuring that our children are as healthy as possible.

Parkfield School recognises that our children come from diverse home backgrounds, cultures, ethnic and faith groups. Our school aims to meet the needs of all children and ensure equality of provision whilst taking account of this diversity and difference.

We understand that some children are 'fussy' eaters and that it is a major step to get some children to eat anything at all. We would want parents to let us know if this is the case so that we can deal with such children sensitively and with encouragement and praise for what they **have eaten**.

Facilities Provided

We will provide a safe, healthy and appealing eating environment for pupils eating packed lunches, and ensure that free fresh drinking water is available at all times. We will encourage all pupils to eat and drink as much of their morning snack or lunch as possible. As fridge space is not available in school parents are advised to send in packed lunches in insulated bags with freezer blocks to keep food fresh.

The school will ensure that eating food from home is a sociable experience where good behaviour and consideration for others is maintained.

We will work with parents/carers to try to ensure that packed lunches contain items of the food groups/Eatwell Plate.

We aim to ensure that all Packed Lunches include:

- At least one portion of fruit (e.g. small apple, orange, grapes, dried fruit, cherry tomatoes) included each day.

- At least one portion of vegetables (e.g. carrot sticks, cucumber, celery) included each day
  .
- Meat, fish or other source of non-dairy protein (eg chicken, turkey, beef, ham, salmon, tuna, lentils, kidney beans, chickpeas, hummus and falafel) included each day.

- Starchy foods such as any type of bread, pasta, rice, couscous, noodles, potatoes or other type of cereals every day (e.g. pitta bread, tortilla wraps, rice cakes, oat cakes) included each day .

- Dairy food such as milk, cheese, yoghurt, fromage frais or custard is included each day.

- Only **one small** sweet snack or cake should be included.

- Drinks should be water, fruit juice, semi-skimmed or skimmed milk, yoghurt or milk drinks and smoothies.

- A paper napkin and eating utensils if necessary.

What is not allowed in School

- Nuts and nut products (e.g. peanut butter) should never be sent to school because of allergy concerns. Neither are children allowed to share food items because of allergy risks.

- Crisps or other such snacks (Quavers, Skips etc) but instead seeds, savoury crackers, breadsticks etc.

- Fizzy drinks and drinks in glass bottles or ring pull cans.

- Chocolate or sweets.

- Hot takeaway food.

Implementation

On a daily basis the staff in school see what children have in their lunchboxes as a matter of course as we are supervising in the hall. This is an opportunity for them to talk with the children about their lunchboxes and to encourage healthy eating and drinking.

At no time will a child be made to feel ashamed of their lunchbox contents.

However, we may send parents a reminder of this policy if lunchbox contents **regularly** fall short of the expectations in this policy. It is not our intention to tell parents what and how they should be feeding their children and we will not do so, but we want to work with parents to educate our children about healthy dietary choices so that they can make their own informed choices independently when they are older.

If your child has not eaten enough of their lunch, we will wrap it up and send it home in their lunch box in order for you to see.

Forgotten Lunch boxes

On occasion children have left lunch boxes at home or in their parent/carer's cars. As soon as this is discovered we will follow these procedures:

- Inform the office and the child's parents will be contacted and asked to bring in the lunchbox.

- If we are unable to reach a parent we will continue to contact other agreed contact names on the child's file.

- If in emergency cases a parent/carer is unable to bring a meal to school, the school, with the parent's permission, will provide the child with a school lunch which will need to be paid for in the school office at the end of the day.

Packed lunch ideas

These ideas below are recommended by the British Nutrition Foundation:

- Tortilla wrap and grilled chicken, lettuce and red pepper slices
- Cherry tomatoes
- Banana
- Fruit fromage frais
- Carton of apple juice
- Rice, bean and meat salad (boiled rice, kidney beans, green beans and chopped
- meat) with a little olive oil and lemon juice
- Peach or nectarine
- Low fat fruit yoghurt
- Slice of banana bread
- Bottle of water
- Granary roll with tinned salmon, lettuce and cucumber
- Sticks of sweet pepper
- Peach or nectarine
- Carton of semi-skimmed milk
- Couscous salad with grilled chicken, chopped peppers and sultanas
- Small tub of fruit cocktail in juice
- Fruit fromage frais
- Bottle of water
- Tuna and pasta salad with tinned tuna, chopped peppers and a little olive oil and lemon juice
- Banana
- Handful of raisins
- Small slice of flapjack
- Carton of semi-skimmed milk
- Pasta and salmon salad (boiled pasta, tinned or grilled salmon and chopped
- cucumber)
- Carrot sticks
- Small tub of fruit cocktail in juice
- Banana smoothie (banana, low fat yoghurt and orange juice)
- Tortilla wrap with mixed beans, grated cheese, lettuce and a little soured cream
- or reduced fat crème fraiche

- Handful of grapes and strawberries
- Fruit fromage frais
- Carton of apple juice
- Boneless chicken
- Potato salad with reduced calorie dressing (homemade or bought)
- Cucumber and carrot sticks
- Banana
- Low fat yoghurt
- Bottle of water
- Mini pittas and houmous, cucumber and grated carrot
- A slice of cheese
- Handful of strawberries or cherries
- Carton of mixed fruit juice
- Wholemeal sandwich with sliced beef, egg, lettuce and tomato
- Sugar snap peas
- Satsuma
- Fruit scone
- Bottle of drinking yoghurt
- Celery and cucumber sticks
- Low fat rice pudding
- Bottle of water

Promotion & Sharing of this Policy

We will inform parents and carers and pupils of the policy via letter, the school newsletter and the school website, including ideas for a healthy lunch box.

Parkfield Community School
May 2016

Parkfield Community School
Administration of Medication

Policy Statement

Parkfield Community School asks that parents request that their doctor, wherever possible, prescribe medication, which can be taken outside the school day.

Parkfield School does **not** administer medication (other than for life threatening conditions). Parents are always welcome to come into school to administer medication to their child.

Children with Special Medical Needs

Should Parkfield School be asked to admit a child to school with medical needs we will, in partnership with the parents/carers and School Nurse, discuss individual needs and if necessary a Health Care Plan will be put in place.

Where appropriate an individual alert card will be developed in partnership with the parents/carers and School Nurse and any resulting training needs will be met.

On Admission to School

All parents/carers will be asked to complete an admissions form giving full details of child's medical conditions, regular medication, emergency medication, emergency contact numbers, name of family doctor, allergies and special dietary requirements etc.

Administration & Storage of Medication in School

Only medication for life threatening conditions will be kept within school ie Epi Pens, Piriton and Asthma Inhalers.

Should there be a life threatening incident where an Epi Pen or Piriton is required then this will be administered by a First Aider and a Medical Emergency Report will be completed

Should the child be required, or is able to administer their own medication, e.g. reliever inhaler for asthma, we will want to ensure they understand their responsibilities in this area. We may want to ask the School Nurse to check the child's technique before accepting full responsibility.

Storage & Disposal of Medication

A regular check will be made of the medication cabinet at least termly, and parents will be asked to collect any medication which is out of date or not clearly labelled. If parents/ carers do not collect this medication it will be taken to the local pharmacy for disposal.

Two supplies of all emergency medication will be kept in Parkfield School where possible. One in the medicine cabinet in the School Office and one kept with the child at all times in the child's classroom (but out of reach of pupils). Staff will be notified of the location of emergency medicines via the medical needs board situated in the staff room.

School Trips

It may be necessary to administer medication to pupils whilst on school trips.
In general, pupils with medical needs will not be excluded from school trips unless there are sound medical or health and safety reasons.

Before taking children off the school premises, the member of staff in charge will check that any medication or equipment that needs to accompany pupils is safely packed.

In more complex cases, and where Health Care Plans are in operation, the Group Leader will have familiarised themselves with the details contained within their plan. Where appropriate, emergency contact details (especially for children with a Health Care Plan) must accompany each member of staff on each visit away from school.

Wherever possible but especially in Key Stage 2 (Years 3 – 6), asthma inhalers will remain the responsibility of the pupil. The member of staff in charge of the trip will check to ensure that asthma inhalers are being carried by those who need them before leaving school.

Residential Trips

Once again, in general, pupils with medical needs will not be excluded from school trips unless there are sound medical or health and safety reasons.

The administration of both prescribed and non-prescribed medication during the course of a residential trip will be controlled by the parents completing a medical needs form.

Responsibility for the collection and administration of all medicines on a residential trip will be given to a named member of staff accompanying the trip. A separate meeting will be held with families of pupils whose medical needs are subject to an individual Health Care Plan. Where necessary, external health care professionals will also be invited to this meeting to ensure that the child's medical needs can be met by the teaching staff during the residential trip.

In extreme emergencies e.g. an anaphylactic reaction or diabetic coma, certain medicines can be administered or supplied without the direction of a medical practitioner for the purpose of saving life. All staff will be made aware of how to contact persons trained to administer medication in an emergency. Where possible, all staff will be trained (and will have given their permission) to administer emergency medicine for the purpose of saving life.

Health Care Plans

Where a child's medical needs go beyond the normal, the SENCO will convene a meeting to agree a Health Care Plan. Parents, the pupil and professionals from the Local Authorities heath team will be invited to attend this meeting.

Responsibility for drawing up a Health Care Plan rests with the Headteacher in consultation with the SENCO. The Health Care Plan will be child specific and detail:

- Procedures to be followed in an emergency.
- Medication (full drug name and dosage instructions).
- Day to day care – food management and information about blood sugar levels etc.
- Consent and Agreement by:

    - Parents/Carers.
    - The appropriate Health Care Professional.
    - The Headteacher or nominated representative such as the SENCO.
    - The child (if appropriate).

- Staff will not disclose details about a pupil's medical condition without the consent of the parents and, where appropriate, the pupil.
- Where parents, or the pupil, decide not to disclose details of medical conditions, they will be asked to indicate certain aspects of school activity that should not be undertaken such as Physical Education/Swimming. Whether and how much members of the school community should know about a pupil's medical condition is not a matter for the school to decide. However, depending on the circumstances, the school may feel that they cannot safeguard a pupil without sharing information and may wish to add this disclaimer to any agreed Health Care Plan.
- In some cases, and with the support of the parents and pupil, staff will raise awareness of a pupil's medical condition with the rest of the class as this can be helpful both educationally and emotionally. On occasions the school might decide to call on a health care professional to speak to the children about a child's medical condition. However, permission will be sought from both the pupil and parents before a meeting of this kind takes place.
- If at any time a member of staff has concerns over the safety or welfare of a pupil, then the normal safeguarding procedures would take effect.

Duty of Care
When administering life saving medication, there is a legal requirement to exercise reasonable care to avoid injury. Staff who administer or oversee the administration of medication would be considered to be discharging their duty of care 'in loco parentis' i.e. the degree of care exercised as that undertaken by the average careful parent in the same circumstances. Provided the administration of medication is controlled, for instance by following the guidelines of this policy and the parental instructions, the risk of injury will be minimised and the member of staff administering medication may therefore be considered to have exercised reasonable care.

Parkfield Community School
May 2016

To be reviewed May 2019

Parkfield Community School
Medical Emergency Report

Pupil's name:	
Date of birth:	
DETAILS OF INCIDENT	
Date:	
Time:	
What happened e.g. allergic reaction minor or severe; seizure, hypoglycaemic attack (low blood glucose level) faint or collapse:	
Details of treatment given:	
Additional information and comments:	
Ambulance sent for:	**YES/NO**
Name of person completing form:	
Date form completed:	

Parkfield Community School

learning for life

E-Safety

and

Data Security

Policies for ICT Acceptable Use

Author:	**David Williams**	
Date of issue:	**May 2015**	
Reviewed:	**May 2016**	**by: Helena Brzeski**
Next Review Due:	**May 2017**	

Parkfield Academy Trust

CONTENTS

GUIDANCE 4

INTRODUCTION 5

MONITORING 7

BREACHES 8

Incident Reporting 8

ACCEPTABLE USE AGREEMENT: PUPILS - PRIMARY 9

PARENTS LETTER 7

ACCEPTABLE USE AGREEMENT: STAFF, GOVERNORS AND VISITORS 8

COMPUTER VIRUSES 12

DATA SECURITY 13

Security 13

Protective Marking 14

Senior Information Risk Owner (SIRO) 14

Information Asset Owner (IAO) 14

DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY 16

E-MAIL 18

Managing e-Mail 18

Sending e-Mails 19

Receiving e-Mails 19

e-mailing Personal, Sensitive, Confidential or Classified Information 20

EQUAL OPPORTUNITIES 21

Pupils with Additional Needs 21

ESAFETY 22

eSafety - Roles and Responsibilities 22

eSafety in the Curriculum 22

eSafety Skills Development for Staff 23

Managing the School eSafety Messages 23

INCIDENT REPORTING, ESAFETY INCIDENT LOG & INFRINGEMENTS 24

Incident Reporting 24

eSafety Incident Log 24

Misuse and Infringements 25

Flowcharts for Managing an eSafety Incident 25

INTERNET ACCESS 28

Managing the Internet 28

Internet Use 28

Infrastucture 29
MANAGING OTHER WEB 2 TECHNOLOGIES 30
PARENTAL INVOLVEMENT 31
PASSWORDS AND PASSWORD SECURITY 32
Passwords 32
Password Security 32
Zombie Accounts 33
PERSONAL INFORMATION PROMISE 34
PERSONAL OR SENSITIVE INFORMATION 35
Protecting Personal, Sensitive, Confidential and Classified Information 35
Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media 35
SAFE USE OF IMAGES 36
Taking of Images and Film 36
Consent of Adults Who Work at the School 36
Publishing Pupil's Images and Work 36
Storage of Images 37
Webcams and CCTV 37
Video Conferencing 37
SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT & REMOVABLE MEDIA 38
School ICT Equipment 38
Portable & Mobile ICT Equipment 39
Mobile Technologies 39
Removable Media 40
SERVERS 41
SMILE AND STAY SAFE POSTER 42
SOCIAL MEDIA, INCLUDING FACEBOOK AND TWITTER 43
SYSTEMS AND ACCESS 44
TELEPHONE SERVICES 45
WRITING AND REVIEWING THIS POLICY 46
Staff and Pupil Involvement in Policy Creation 46
Review Procedure 46
CURRENT LEGISLATION 47
Acts Relating to Monitoring of Staff eMail 47
Other Acts Relating to eSafety 47
Acts Relating to the Protection of Personal Data 49
APPENDIX 50

Information Risk Actions Form 50
School Policy in Brief 51

Guidance

The following sections contain much **guidance** for the acceptable use of ICT at Parkfield Community School. It is intended for staff and pupil use.

This policy has been ratified by the School's Governors and has then been made available to all personnel, including Governors, staff and pupils, involved in the working of the school.

Rights Respecting School Link: A17: *Every child has the right to reliable information from the mass media in a way that they can understand. Governments must help protect children from materials that could harm them.*

Introduction

ICT 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 our young people with the skills to access life-long learning and employment.

Information and Communications Technology 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 both inside and outside of the classroom include:

- websites
- e-mail, Instant Messaging and chat rooms
- social media, including Facebook and Twitter
- mobile/ smart phones with text, video and/ or web functionality
- other mobile devices with web functionality
- gaming, especially online
- Learning platforms and virtual learning environments
- blogs and wikis
- podcasting
- video broadcasting
- music downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, 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, usually 13 years.

At Parkfield Community School, we understand the responsibility to educate our pupils on e-safety 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, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation 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. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice

ICT authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, 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 school ICT; 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.

ICT authorised staff may, without prior notice, access the e-mail where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

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

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The ICO's new powers to issue monetary penalties came into force on 6 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

Non-compliance with this policy, along with all security breaches or attempts, unsolicited emails, loss of/theft of equipment/data and any unauthorised use or suspected misuse of ICT must be immediately reported to the school’s SIRO (Senior Information Risk Owner – Hazel Pulley).

All virus notifications should be reported to the ICT technician team immediately and the offending device should not be used until this advice has been sort.

Please refer to the relevant section on Incident Reporting, e-safety Incident log & Infringements.

Acceptable Use Agreement: Pupils - Primary

Primary Pupil Acceptable Use
Agreement/e-safety Rules

- I will only use ICT in school for school activities and to complete homework.
- I will only use my own school e-mail address on school computers.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will keep my ICT passwords from other children.
- I will only open/delete my own files.
- I will be polite and sensible when using ICT at all times.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I accidentally find anything that makes me feel uncomfortable online, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address to anyone, because this is dangerous.
- I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my e-safety.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

School Council Leader's Signature - ___________________

Dear Parent/ Carer

ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT equipment.

Please read and discuss these e-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your child's class teacher.

Thank you for your continued support.

Yours sincerely,

Mr Williams
Assistant Headteacher and e-safety co-ordinator

- - ✂ -

To Parkfield Community School

We have discussed this and ……………………………………………(child name) agrees to follow the e-safety rules and to support the safe use of ICT at Parkfield Community School.

Parent/ Carer Signature ………………………….…………………………

Class …………………………………. Date ………………………………

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with David Williams (school e-safety) coordinator or Hazel Pulley Senior Information Risk Owner (SIRO).

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT 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 are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of Hazel Pulley (headteacher), David Williams (ICT co-ordinator), Richard Heeley (network manager). Apps may however be downloaded on staff Ipads for school related purposes without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with 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, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

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

Signature …….…………………….………… Date ……………………

Full Name ………………………………..(printed)

Job title ……………………………………………………..………

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment that you use.

- All school laptops should be connected to the school network **AT LEAST ONCE A MONTH** to ensure that anti-virus software is updated.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact Richard Heeley immediately if you are at school, or at the first available opportunity when an incident occurs at home. They will advise you what actions to take and will be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The school is aware of the Becta guidelines found at

http://tinyurl.com/76gj9xr

and the advice and guidance given by the Information Commissioner's Office (ICO)

http://www.ico.gov.uk/for_organisations/data_protection/security_measures.aspx

Security

- The school gives relevant staff access to its Management Information System, with differentiated levels of access and a unique username and password.
- It is the responsibility of everyone to keep their passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
- Staff have read the relevant guidance documents concerning 'Safe Handling of Data' .
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO).
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Access to staff email accounts is protected by a passcode pin on all personal devices.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents
- Parkfield Community School uses 3 levels of labelling
  - Public (or if unmarked) – this will imply that the document contains no sensitive or personal information and will be a public document. All staff have access
  - Private – this is private to the person who attaches.
  - Confidential – documents for admin staff and senior management only.
- These restrictions are applied through a series of stampers and through automatic header and footers notices through MIS generated reports.

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response. The SIRO has the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

The SIRO in this school is Hazel Pulley.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Please refer to the appendix at the back of this document showing examples of information assets a school may hold.

The role of an IAO is to understand:

- what information is held, and for what purposes;
- what information needs to be protected how information will be amended or added to over time;
- who has access to the data and why;
- how information is retained and disposed off.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

The IAO in this school is Lisa Davies.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed off through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

- Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998
http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

- The school's disposal record will include:
    - Date item disposed of
    - Authorisation for disposal, including:
        - verification of software licensing
        - any personal data likely to be held on the storage media?
    - How it was disposed of eg waste, gift, sale
    - Name of person & / or organisation who received the disposed item

- If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

http://www.ico.gov.uk/

Data Protection Act – data protection guide, including the 8 principles

http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

e-mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette;‘netiquette’.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. **The school email account should be the account that is used for all school business**.

- **Under no circumstances** should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

- All school e-mails have a standard disclaimer attached to them, stating that, ‘the views expressed are not necessarily those of the school'.

- All personal devices, which automatically access school e-mail accounts are password protected.

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  – Delete all e-mails of short-term value;
  – Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.

- All pupils in Years 5 and 6 have their own school e-mail accounts. Children are only able to send e-mails from these accounts to others within the Parkfield network of e-mail addresses.

- The forwarding of chain letters is not permitted in school.

- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

- Staff must inform (the e-safety co-ordinator or line manager) if they receive an offensive e-mail.

- Pupils are introduced to e-mail as part of the ICT Scheme of Work, and relevant skills and 'netiquette' are taught and reinforced.

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending e-Mails

If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section

- e-mailing Personal, Sensitive, Confidential or Classified Information.

- Use your own school e-mail account so that you are clearly identified as the originator of a message.

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

- **School e-mail is not to be used for personal advertising**.

Receiving e-Mails

- Check your e-mail regularly.

- Never open attachments from an untrusted source; Consult your network manager first.

- The automatic forwarding and deletion of e-mails is not allowed.

e-mailing Personal, Sensitive, Confidential or Classified Information

- Where possible sensitive information should not be sent via e-mail. If your conclusion is that e-mail must be used to transmit such data, then please ensure that the following points are followed:

  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address, of any intended recipient of the information.
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary .

  - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone).
  - Request confirmation of safe receipt.

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

e-safety

e-safety - Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinator in this school is *(David Williams)* who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

e-safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- The school has a framework for teaching internet skills in ICT/ PSHME lessons.

- The school provides opportunities within a range of curriculum areas to teach about e-safety.

- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum.

- Pupils are aware of the relevant legislation when using the internet, such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation, such as Cybermentors, Childline or CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

eSafety Skills Development for Staff

- Our staff receive regular information and training on e-safety. They then promote the 'Stay Safe' online messages in the form of lessons, modeling and guidance e.g. through the use of Moodle.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts)
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas

Managing the School e-safety Messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils and staff at the start of each school year.
- E-safety posters will be prominently displayed.
- The key e-safety advice will be promoted widely through school displays, newsletters, class activities and so on.

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO or e-safety co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner. See Page 14.

e-safety Incident Log

At Parkfield Community School we keeping an incident log to monitor what is happening and ot identify trends or specific concerns. See next page.

All e-safety concerns will be recorded by the SEAL team, who will then inform the e-safety co-ordinator and/or SIRO of the incident. This log will be kept in the SEAL room and will be monitored termly by the Headteacher, Member of SLT or Chair of Governors.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to e-safety should be made to the e-safety co-ordinator or Headteacher. Incidents should be logged and **Flowcharts on the next page for managing an e-safety incident** should be followed.

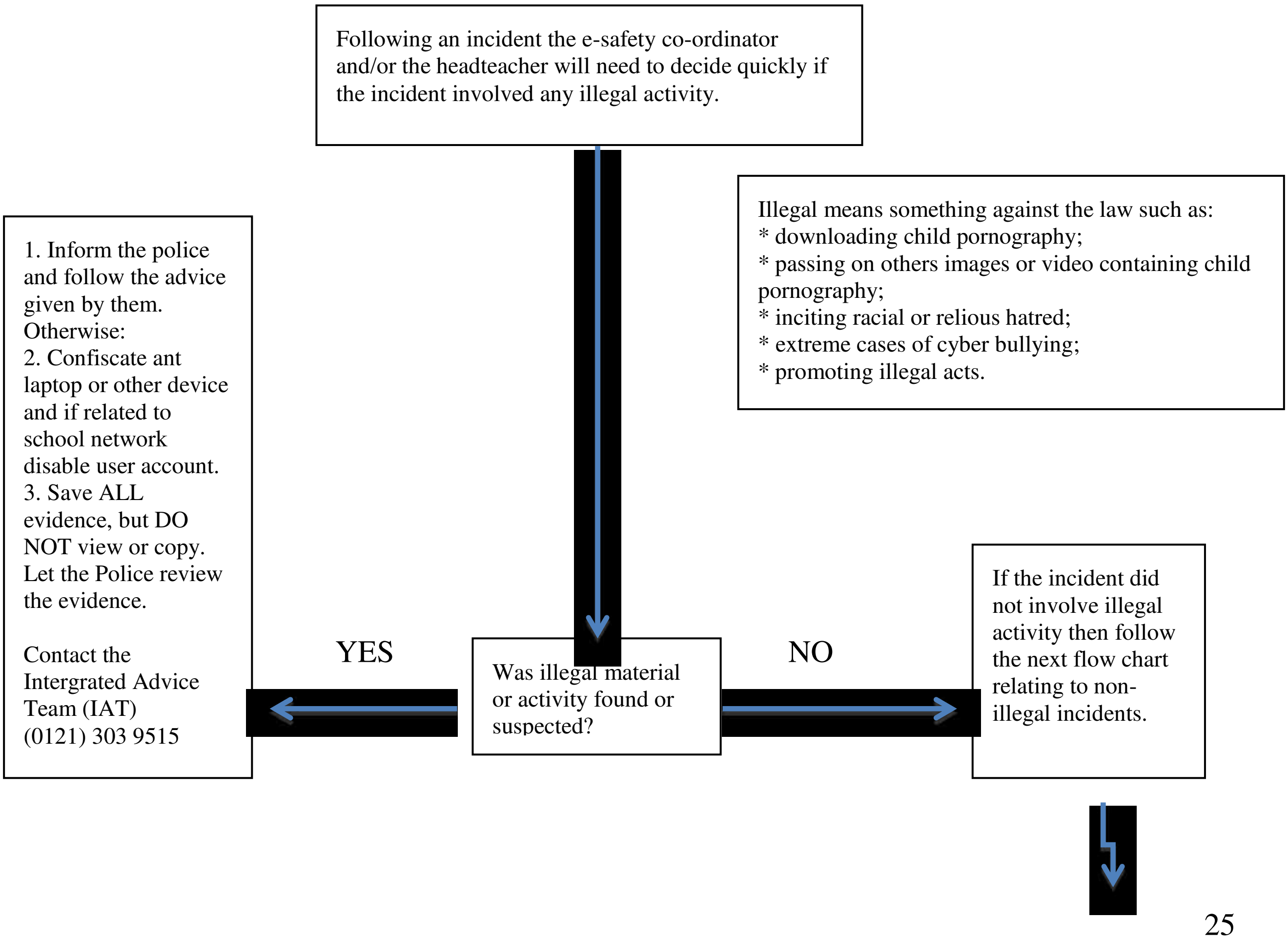
Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).
- Users are made aware of sanctions relating to the misuse or misconduct and action will be taken in line with our disciplinary policy.

Flowcharts for Managing an e-safety Incident

Flowchart to support decisions related to an illegal eSafety incident

For Headteachers, Senior Leaders and e-safety co-ordinators



Following an incident the e-safety co-ordinator and/or the headteacher will need to decide quickly if the incident involved any illegal activity.

Illegal means something against the law such as:
* downloading child pornography;
* passing on others images or video containing child pornography;
* inciting racial or relious hatred;
* extreme cases of cyber bullying;
* promoting illegal acts.

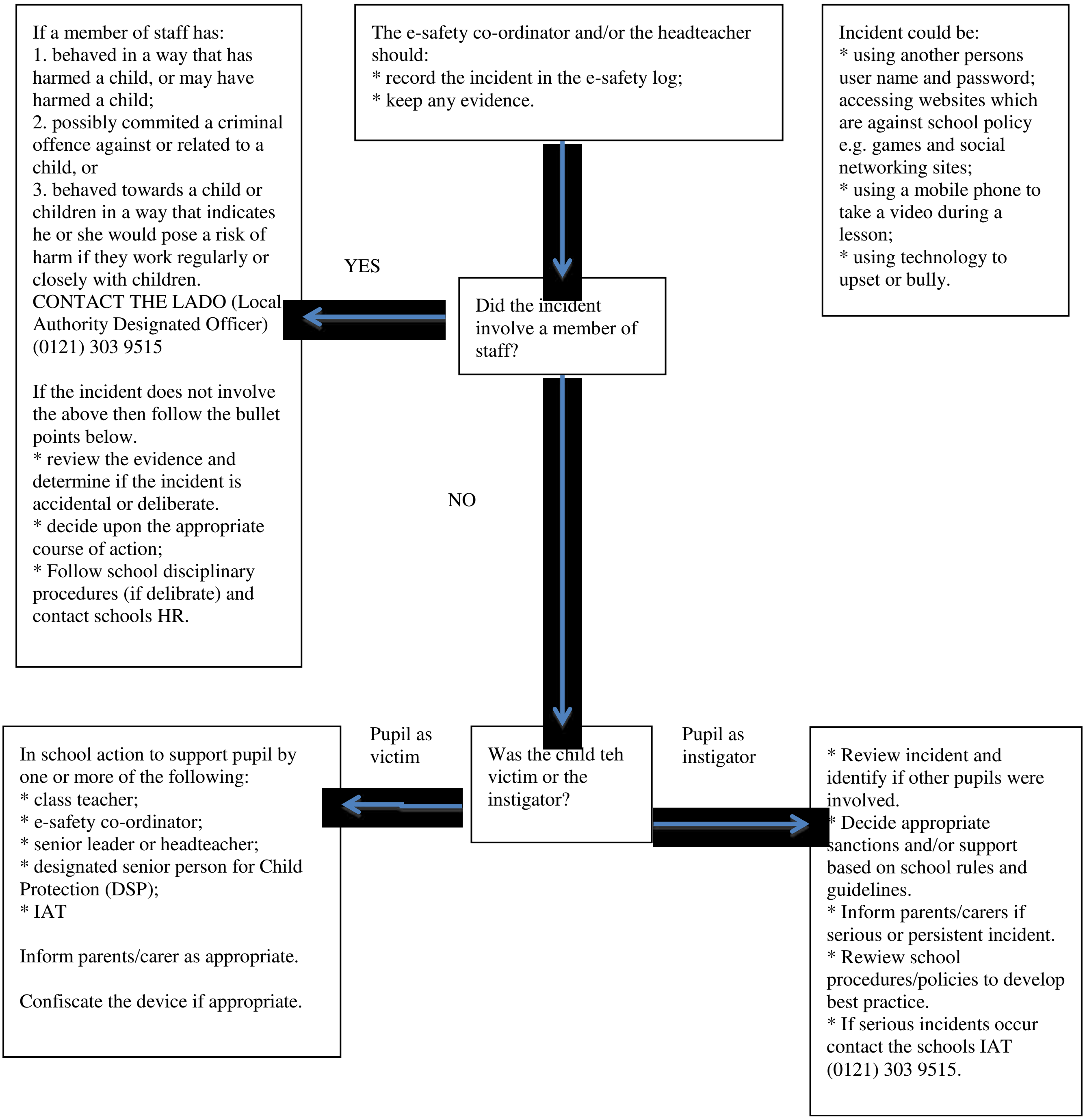
Was illegal material or activity found or suspected?

1. Inform the police and follow the advice given by them.
Otherwise:
2. Confiscate ant laptop or other device and if related to school network disable user account.
3. Save ALL evidence, but DO NOT view or copy. Let the Police review the evidence.

Contact the Intergrated Advice Team (IAT)
(0121) 303 9515

If the incident did not involve illegal activity then follow the next flow chart relating to non-illegal incidents.

Follow this flow chart if illegal activity did not occur.



The e-safety co-ordinator and/or the headteacher should:
* record the incident in the e-safety log;
* keep any evidence.

Incident could be:
* using another persons user name and password; accessing websites which are against school policy e.g. games and social networking sites;
* using a mobile phone to take a video during a lesson;
* using technology to upset or bully.

Did the incident involve a member of staff?

YES

If a member of staff has:
1. behaved in a way that has harmed a child, or may have harmed a child;
2. possibly commited a criminal offence against or related to a child, or
3. behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.
CONTACT THE LADO (Local Authority Designated Officer) (0121) 303 9515

If the incident does not involve the above then follow the bullet points below.
* review the evidence and determine if the incident is accidental or deliberate.
* decide upon the appropriate course of action;
* Follow school disciplinary procedures (if delibrate) and contact schools HR.

NO

Was the child teh victim or the instigator?

Pupil as victim

In school action to support pupil by one or more of the following:
* class teacher;
* e-safety co-ordinator;
* senior leader or headteacher;
* designated senior person for Child Protection (DSP);
* IAT

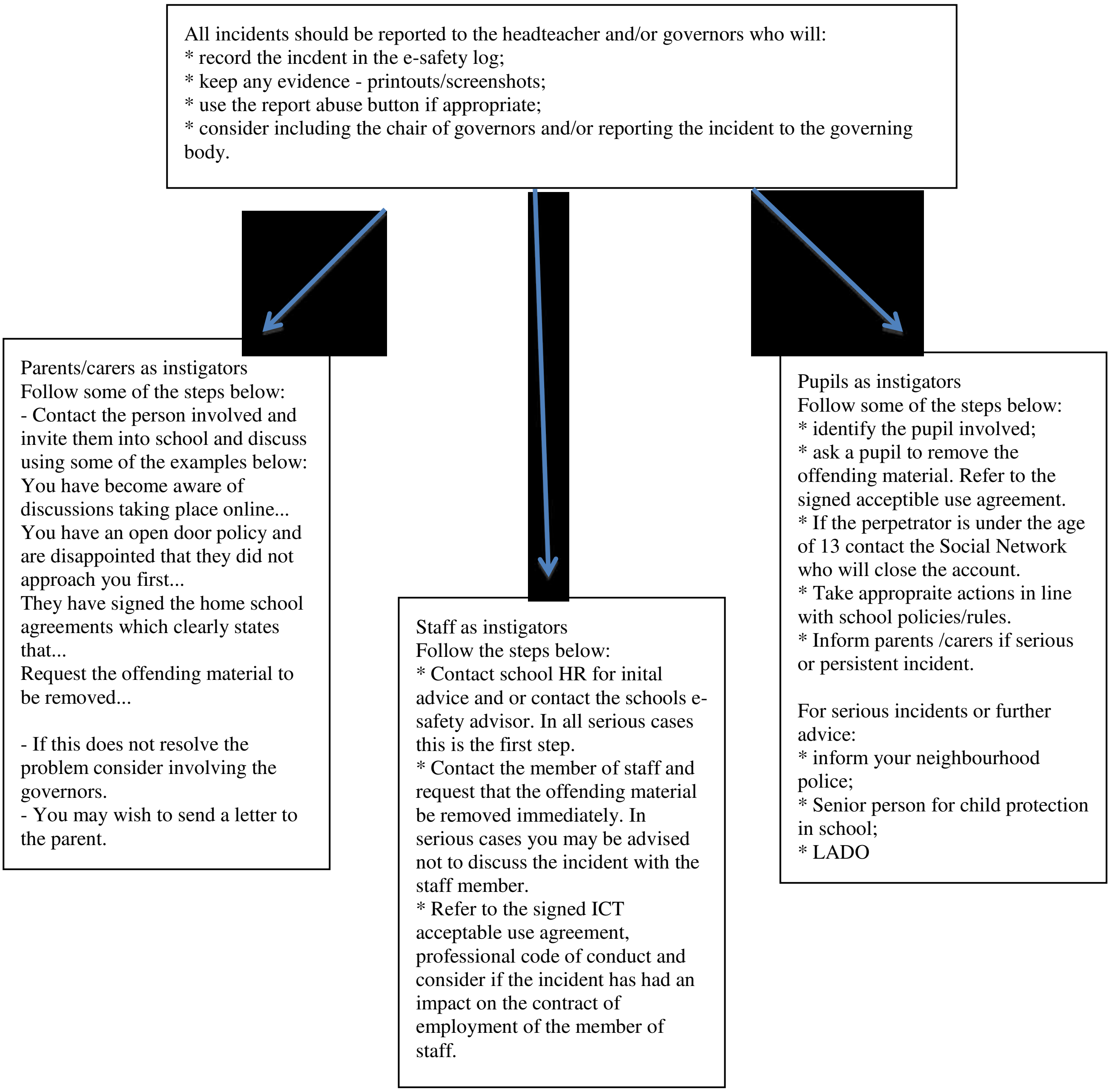
Inform parents/carer as appropriate.

Confiscate the device if appropriate.

Pupil as instigator

* Review incident and identify if other pupils were involved.
* Decide appropriate sanctions and/or support based on school rules and guidelines.
* Inform parents/carers if serious or persistent incident.
* Rewiew school procedures/policies to develop best practice.
* If serious incidents occur contact the schools IAT (0121) 303 9515.

Use the following flow chart if staff are victims



All incidents should be reported to the headteacher and/or governors who will:
* record the incdent in the e-safety log;
* keep any evidence - printouts/screenshots;
* use the report abuse button if appropriate;
* consider including the chair of governors and/or reporting the incident to the governing body.

Parents/carers as instigators
Follow some of the steps below:
- Contact the person involved and invite them into school and discuss using some of the examples below:
You have become aware of discussions taking place online...
You have an open door policy and are disappointed that they did not approach you first...
They have signed the home school agreements which clearly states that...
Request the offending material to be removed...

- If this does not resolve the problem consider involving the governors.
- You may wish to send a letter to the parent.

Staff as instigators
Follow the steps below:
* Contact school HR for inital advice and or contact the schools e-safety advisor. In all serious cases this is the first step.
* Contact the member of staff and request that the offending material be removed immediately. In serious cases you may be advised not to discuss the incident with the staff member.
* Refer to the signed ICT acceptable use agreement, professional code of conduct and consider if the incident has had an impact on the contract of employment of the member of staff.

Pupils as instigators
Follow some of the steps below:
* identify the pupil involved;
* ask a pupil to remove the offending material. Refer to the signed acceptible use agreement.
* If the perpetrator is under the age of 13 contact the Social Network who will close the account.
* Take appropraite actions in line with school policies/rules.
* Inform parents /carers if serious or persistent incident.

For serious incidents or further advice:
* inform your neighbourhood police;
* Senior person for child protection in school;
* LADO

Internet Access

The internet is an open worldwide communication medium, 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, business and social interaction, as well as a potential risk to young and vulnerable people. The school uses the LA web filtering system which prevents access to a range of inappropriate sites and searches. This is also supplimented through the use of policy central which logs any inappropriate internet search activity. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Users must not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application.
- It is strongly recommended that staff with social networking accounts, such as Facebook have their accounts the privacy settings engaged to prevent access by the local community and children.
- On-line gambling or gaming is not allowed.

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastucture

- School internet access is controlled through the LA’s web filtering service.

- Policy Central is used to identify any words or phrases that are inputted or searched for. Screen captures of incidents are then automatically emailed to the headteacher, network manager and e-safety co-ordinator.

- Parkfield Community School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

- The school uses management control tools for controlling and monitoring workstations.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.

- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school’s responsibility nor the network manager’s to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the ***(technician/teacher)*** for a safety check first.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from ***(the Headteacher/technician/ICT subject leader).*** Staff may however install apps onto school owned iPads as long as they are for educational purposes.

- If there are any issues related to viruses or anti-virus software, the network manager (Richard Heeley) should be informed as soon as possible.

Managing Other Web 2 Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, 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 pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school.

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

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

- Pupils 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 numbers, school details, IM/ email address, specific hobbies/ interests).

- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.

- Our pupils are asked to report any incidents of Cyberbullying to the school.

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher.

Parental Involvement

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

- Parents/carers are regularly invited to attend e-safety briefings in school.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).
- Parents/carers are expected to sign a Home School agreement containing the following statement or similar "**We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community."**
- The school disseminates information to parents relating to e-safety where appropriate in the form of:
    - Posters
    - School website
    - Newsletter items

Passwords and Password Security

Passwords

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- If passwords or encryption keys are recorded on paper or in a computer file, these should be in a secured location (or in a password protected file).
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- **Never tell a child or colleague your password.**
- **If you aware of a breach of security with your password or account inform Richard Heeley immediately.**
- Where possible passwords should contain a minimum of six characters and be difficult to guess. It is also advisable that they also contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the school are removed from the system within 48 hours.

If you think your password may have been compromised or someone else has become aware of your password report this to the ICT support team.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email, learning platform and Management Information System (where appropriate) log-in username. From

Year 2 they are also expected to use a personal password and keep it private

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 18:00.

- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)

- In our school, all ICT password policies are the responsibility of **Richard Heeley** and all staff and pupils are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

Zombie accounts are therefore disabled once the member of the school has left (within 48 hours).

Personal Information Promise

The Information Commissioner's Office launched a Personal Information Promise in January 2009. Schools may wish to sign up to this promise which is shown below.

The personal information promise is:

I Hazel Pulley (Headteacher) on behalf of Parkfield Community School promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing

More information available -

http://www.ico.gov.uk/upload/documents/pressreleases/2009/personal_information_promise_280109.pdf

To view the promise

http://www.ico.gov.uk/upload/documents/personal_info_promise/pip%20final.pdf

To sign the promise

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/personal_information_promise.aspx

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

Staff at Parkfield Community School:

- ensure that any school information accessed from their own PC or removable media equipment is kept secure;
- ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others;
- ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person;
- ensure the security of any personal, sensitive, confidential and classified information contained in documents they fax, copy, scan or print.
- only download personal data from systems if expressly authorised to do so by their manager;
- do not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- keep keep screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

Staff at Parkfield Community School:

- ensure removable media is purchased with encryption;
- store all removable media securely;
- securely dispose of removable media that may hold personal data;
- encrypt all files containing personal, sensitive, confidential or classified data;
- ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site;
- in the school prospectus and other printed publications that the school may produce for promotional purposes;
- on the school's learning platform or Virtual Learning Environment;
- in display material that may be used in the school's communal areas;

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only Richard Heeley and David Williams have authority to upload to the site.

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 pupils within the confines of the school network or other online school resource;
- ***Richard Heeley*** has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this, with appropriate cause, are **Richard Heeley, members of the school leadership team and the building site supervisor.** Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document).
    - Webcams can be found ***built in to any Macs in school, on Ipads and on some netbooks.***

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences.
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing.
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- Approval from the Headteacher is sought prior to all video conferences within school.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity.
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- Ensure that all ICT 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.
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of 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 ICT equipment should not be used on a school network without the permission of the headteacher, ICT Co-ordinator or ICT technicial support team.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.
- 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 ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
  - maintaining control of the allocation and transfer within their Unit;
  - recovering and returning equipment when no longer needed.

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

- Portable equipment must be transported in its protective case if supplied.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies, such as: Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- 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 devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices

- The sending of inappropriate communications between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '**Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media**' - Page 35

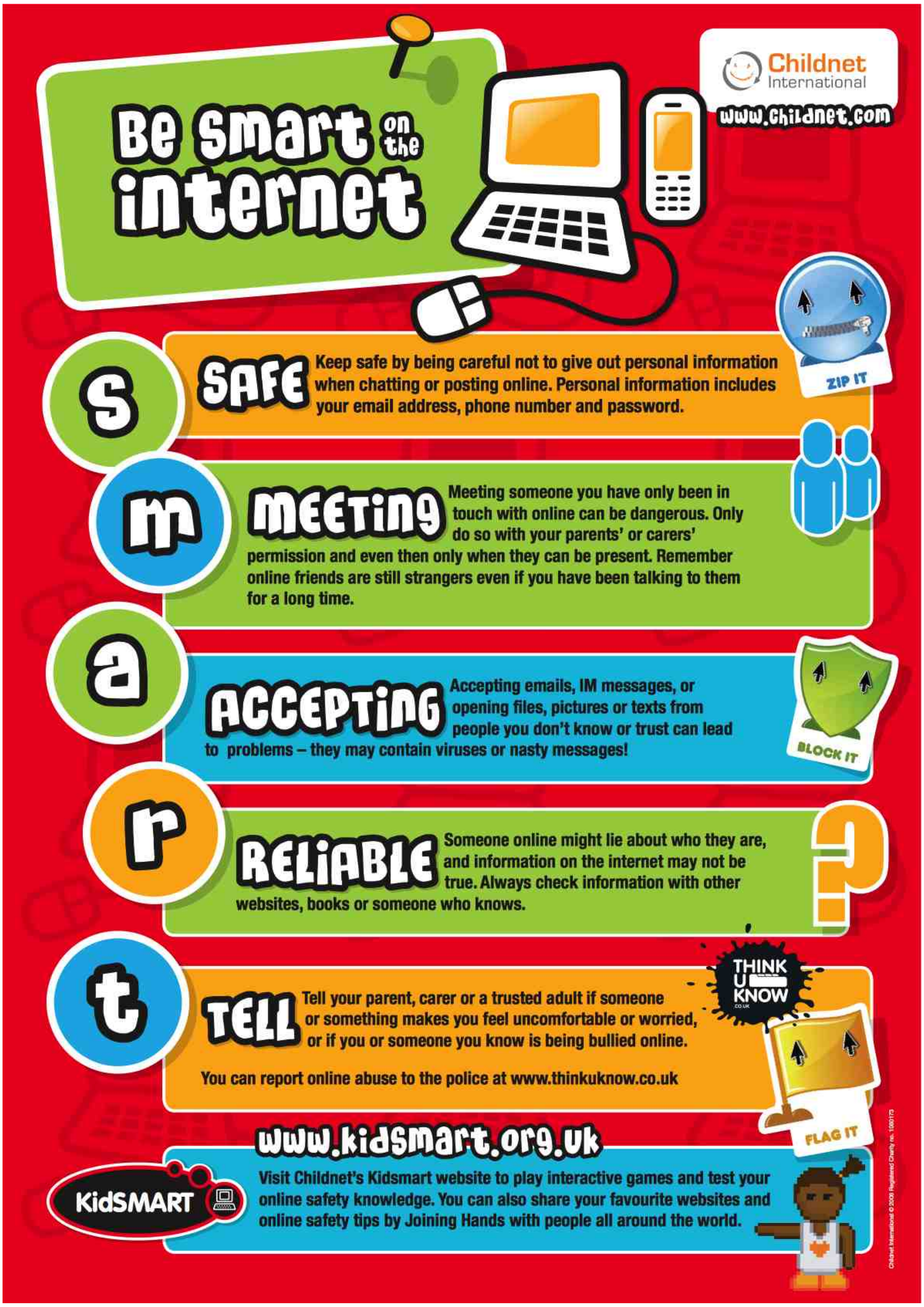
- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect - see Page 35
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

- Always keep servers in a locked and secure environment.
- Limit access rights.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine’s specification.
- Data must be backed up regularly.
- Back up media must be securely stored in a fireproof container.
- Back up media are encrypted off-site and in the ICT support teams office.
- Remote back ups should be automatically securely encrypted.

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school



Be smart on the internet

S SAFE Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Childnet International © 2008 Registered Charity no. 1080173

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Twitter to communicate with parents and carers. Richard Heeley is responsible for all postings on this technology and monitors responses from others.

- Staff ***are not*** permitted to access their personal social media accounts using school equipment ***during school hours***.

- Staff with online social media accounts must ensure that they are locked down fully to prevent access to them by pupils/the local community.

- Under no circumstances are staff to befriend pupils (past or present) on social networking sites, such as Facebook.

- Pupils are not permitted to access their social media accounts whilst at school.

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC.

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided by the school (without suitable supervision).

- Use **ONLY** your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.

- Do not introduce or propagate viruses.

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on school systems, hardware or used in relation to school business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Telephone Services

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others;

    2. They are not for profit or to premium rate services;

    3. They conform to school policies;

    4. They are routed through the main office, who will deem their importance if you are unavailable.

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

- Ensure that your incoming telephone calls, to personal phones, can be handled at all times.

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

- Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through consultation, governing body meetings and through the school council.

Review Procedure

There will be on-going opportunities for staff to discuss with the e-safety coordinator any e-safety issue that concerns them.

There will be on-going opportunities for staff to discuss with the SIRO/AIO any issue of data security that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, head teacher and governors on

Head teacher's signature - ________________________ Date ______________

Chair of Governor's signature - ____________________ Date ______________

E-Safety Co-ordinators signature - _________________ Date ______________

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from*

Sexual Crime" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Appendix

Information Risk Actions Form

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Appendix 2

School Policy in Brief

- At this school we have an Acceptable Use policy/agreement which is reviewed at least annually, which all staff/visitors/Governors sign. Copies are kept on file.

Protect and Restricted material/data must be encrypted, if the material is to be removed from the school.

- At this school teachers are supplied with automatically encrypted flash drives for this purpose. Visitors and supply teachers are not permitted to remove any protected or restricted materials from the school site without the Headteacher's approval.
- At this school we securely transfer CTF pupil data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer.
- Sensitive material in non digital formats, such as paper and stamped and should be stored in a secure place.
- At ths school all servers are managed by CRB-checked staff.
- At this school we use follow LA back-up procedures and back up our curriculum server to a secure location in school.
- At this school we use an onsite and off site recovery for our admin server. Backed up files on site are kept in a secure location.

Disposal: Sensitive or personal material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At this school we use a deposal company, that follows LA guidelines, for the disposal of system harddrives where any protected or restricted data has been held.
- At this school paper based sensitive information is shredded.
- Laptops used by staff at home (loaned by the school) are brought in and disposed of through the same procedure.
- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, SLG and Learning Platform access are controlled by Richard Heeley.
- Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation.

Parkfield Community School Gender Equality Policy

Links to Rights Respecting: A29: *Education should encourage understanding, peace, tolerance, equity of sexes and friendships among all peoples, ethnic, national and religious groups.*

Legislative Context

The Equality Act (2006) amended the requirements of the Equal Pay Act (1970) and the Sex Discrimination act (1975). It added to the duty to eliminate sexual discrimination and sexual harassment, the duty to promote gender equality.

Social Context

We understand that despite thirty years of individual legal rights to sex equality there is still widespread discrimination and persistent gender inequality. Both sexes suffer from the stereotyping of their roles and needs and such stereotyping has to be understood, challenged and overcome.

School Mission Statement

At Parkfield Community School we aim through our school values for all, to learn and achieve to an outstanding level in a safe and happy environment.

The General Duty

In accordance with our school's mission statement and values, we welcome the statutory Gender Equality Duty. In compliance with the General Duty, Parkfield Community School has due regard for the need to, and works to:

- Eliminate unlawful sexual discrimination.
- Eliminate sexual harassment.
- Promote gender equality.

By unlawful sexual discrimination we mean treating one person less favourably than another on grounds of sex or gender. We understand that this could be done directly but that it could also occur indirectly. Indirect discrimination means that a particular policy or practice may impact more negatively on one gender than on the other, or may favour one gender to the disadvantage of the other.

By sexual harassment we refer to behaviour or remarks based on a person's sex or gender, perceived to be unpleasant, threatening, offensive or demeaning to the dignity and self-esteem of the recipient or subject, we see behaviour as also damaging to the perpetrator. (Refer further: our school's Behaviour/Anti Bullying policy).

We understand 'sex' to refer to the biological differences between males and females and 'gender' to refer to the wider social roles and responsibilities which structure our lives. By promoting gender equality our intention is to recognize and help overcome those lasting and embedded patterns of advantage and disadvantage which are based on socially ascribed gender stereotypes and assumptions.

We understand that in some circumstances it may be appropriate to teat girls and boys, and women and men differently, if that action is aimed at overcoming previous, current or possible future disadvantage.

We will take steps to counteract the effects of any past discrimination in staff recruitment. Where we are uncertain whether there is a genuine occupational requirement for preference to be given to the employment of someone of a particular gender we will seek specialist advice.

We understand the three parts of the duty to be different, but that they should normally support each other. However, we are aware that achieving one may not lead to achieving all three.

In taking due regard we will exercise the principles of proportionally and relevance. By this we mean that the weight we give to gender equality will be proportionate to its relevance to a particular function. The greater the relevance of a function to gender equality, the greater regard we will pay to it.

The Specific Duties

We welcome the responsibility to think and act more strategically about gender equality. To meet the specific duties, and guided by the Code of Practice prepared by the Equal Opportunities Commission, we have prepared, published and implemented, and will maintain a Gender Equality Action Plan which contains our current objectives, This is attached to and forms an essential part of this policy.

We are working to develop our understanding of the major gender equality issues in our school's functions and services. In order to do this we:

- Collect and analyse school data and other gender equality relevant information, including data about our local area.
- Consult all staff, pupils, parents and relevant local communities.
- Review all our school policies and practices to assess the ways in which they might impact on gender equality.
- Ensure governors, staff, pupils, parents and others in our school are accountable and understand their responsibilities with regard to preventing discrimination and harassment and promoting gender equality.
- Assess and address the causes of any gender pay gap.
- Publish and implement the Action Plan with our proposed objectives and actions.

We will:

- Set out results of reviews, consultations and impact assessments.
- Report on progress annually and set further objectives where necessary.
- Review and revise the Policy and Action Plan at least every three years.

Responsibilities

All governors, staff, volunteers, pupils and their families need to develop an appropriate understanding of, and act in accordance with, the school's Gender Equality Policy and Action Plan. In addition:

The school governors are responsible for ensuring that the School prepares publishes, implements, reports on and reviews a Gender Equality Policy and Action Plan (including budget requirements), and in particular the employment implications of meeting the Duty.

The Head Teacher works with the Leadership Team to ensure that –

- The Policy and Action plan are implemented.
- Staff recruitment, training opportunities and conditions promote gender equality.
- All staff, pupils and their parents are consulted regarding, and are aware of the school's responsibilities to meet, the Gender Equality Duty.
- Existing and planned policies are assessed for the ways in which they impact on gender equality.
- Curriculum planning, learning and teaching methods, classroom organisation and assessment procedures, behaviour management, school journeys and extended school activities take account of the need to promote gender equality.
- Incidents of sexual/gender bullying or harassment are dealt with according to our Behaviour/Anti Bullying policy.
- Visitors to the school, or those who use the premises, are aware of the Gender Equality policy and action plan.

All staff have a responsibility to deal with incidents of sexual harassment or bullying; help eliminate unlawful discrimination; prepare and/or help deliver a curriculum, learning and teaching methods, classroom organisation and assessment procedures, behaviour management, school journeys and extended school activities (including work with parents) that take account of the need to eliminate unlawful discrimination and harassment and promote gender equality.

Pupils and parents have a proportionate responsibility to understand and act in accordance with the policy, as do **visitors** to the school.

These and other responsibilities are outlined in detail in our Gender Equality Action Plan which is attached to and forms part of this policy.

We believe that, even having the Equal pay Act of 1970 and the Sex Discrimination Act of 1975, there is still widespread discrimination and gender inequity in society. We believe that having this gender equality policy and action plan will:

- Support us in our decision-making and policy development
- Give us a clearer understanding of the needs of staff, pupils and their families
- Enable us to provide better quality services which meet varied needs
- Help us to target our resources more effectively
- Help promote increased confidence in our school
- Make more effective use of workforce.

We recognise that both sexes can suffer from sexual stereotyping and that sometimes the same policies and practices can impact differently on men and women and boys and girls. We will make appropriate adjustments if this is found to be the case with any of our policies and practices.

We also recognise that girls and boys, and women and men, can experience different forms of discrimination depending on, among other thing, their ethnicity, belief, sexual orientation, age or disability and we will take this complexity into consideration.

In these ways we will strive to improve the situation for, and the relationships between, men and women and boys and girls within our school and wider community.

Breaches of the Gender Equality Policy

We understand that eliminating gender discrimination and harassment and promoting gender equality is in part an education function and a matter of cultural change. Where possible, breaches of the policy will be dealt with in a manner appropriate to the level of the breach, and with the intention of bringing about the relevant changes. More serious breaches of this policy will be dealt with in accordance with our school's anti-bullying and harassment procedures, and the disciplinary procedures for staff.

Where safeguarding issues based on sex and gender come to the attention of the school these will be dealt with according to our child protection procedures.

Consultation; publishing; staff, pupils and parent development

This policy has been drawn up in consultation with governors, staff, pupils, parents and members of our local community. These consultations have contributed to developing the awareness among governors, staff, pupils and parents of the ongoing need to eliminate unlawful sexual discrimination and harassment and to promote gender equality.

Copies of this policy are available in the office/public entrance areas of the school, on our website, in staff/department policy folders.

A brief summary of the main points of the policy is made available in age-appropriate ways to our pupils. A summary is printed occasionally in our newsletter, and is available in the home languages of our major ethnic groups.

We will continue, as outlines in our action plan to develop awareness of what constitutes unlawful gender discrimination and harassment, and of the need to eliminate this and to promote gender equality.

May 2016

To be reviewed as necessary