FIVE RIVERS CHILDCARE LTD

Internet Safety Policy & Procedure

'Five Rivers is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment'

Policy Owner	Headteacher
Authoriser	Education Advisor to the Board
Date of Original Issue	01/08/2018
Date of This Issue	01/08/2018
Date of Next Review	01/08/2019
Version	V1

Table of Contents

1. Internet Safety Policy

1.1 Policy Statement

1.1.1 This policy applies to all members of our school community, including staff, pupils, carers, parents, volunteers visitors and all school users who have access to and are users of the school system ICT systems both in and out of school.

1.1.2 The Education and Inspections Act 2006 empowers Head teachers, to such an extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying or other safety incidents covered by this policy, which take place out of school, but is linked to membership of the school.

1.1.3 The Education and Inspections Act 2011 extended the powers included in the 2006 Act and gave permission for Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

1.1.4 Our School will deal with such incidents within this policy and associated behaviour and preventing bullying policies and will, where known inform parents, carers and placing authorities of inappropriate e-safety behaviour that takes place out of school.

1.1.5 Adapted using the South West Grid for learning and the ThinkuKnow programme from CEOPS. This policy should also be read in conjunction with our Safeguarding and Anti-bullying policies.

1.2 Terms and Definitions

1.2.1 The below table sets out a number of terms and definitions used within this document:

Term	Definition
Nil	

1.3 Data Protection

1.3.1 Five Rivers Child Care supports the objectives of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and other legislation relating to Data Processing, including the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and the Freedom of Information Act 2000. Five Rivers Child Care has a statutory obligation to process personal data in accordance with the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

1.3.2 Every member of Five Rivers Child Care has an obligation to ensure that the information they process (use) is collected, maintained and disclosed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and the Five Rivers Child Care Data Protection Policy.

1.4 Disclosure of Information

1.4.1 Any use or disclosure of information held within Five Rivers Child Care, without there being a legitimate purpose or legal basis, will be classed as unauthorised and is a criminal offence under Section 55 of the Act Right of Access (Subject Access Requests).

2.   Internet Safety Procedure

2.1   The internet is a useful tool for pupils and staff at the School as it supports our curriculum and learning opportunities and helps us offer a wider range of subjects, resources and learning opportunities than we would otherwise be able to provide.

2.1.2   New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

2.2   Roles and Responsibilities

2.2.1   The Head Teacher

- The Headteacher is responsible for ensuring the safety (including e-safety) of all members of the school.
- The Headteacher (or delegated team member) will work closely with the Five Rivers ICT manager to regularly monitor the safety of ICT.
- The Headteacher and other designated safeguarding officers within the school will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow diagram *'responding to incidents of misuse')*

2.2.2   The ICT Manager

- The ICT manager is responsible for ensuring that the school's ICT infrastructures are secure and not open to misuse or malicious attack
- Must ensure that the school's e-safety technical requirements meet with requirements outlined in the Childrens Internet Protection Act, CIPA (from Objective's Jason Pine)
- The manager must ensure that users may only access the school's networks through properly enforced password protection policy, in which passwords are regularly changed.
- Will ensure that the school's filtering system is regularly updated
- Must keep up to date with e-safety technical information in order to effectively carry out their e-safety duties.

2.2.3 Teaching and Support Staff

- Must ensure they have an up to date awareness of e-safety matters and of current school e-safety policies and practices
- Have read, understood and signed the school staff Acceptable Use Policy/Agreement (AUP)
- Are responsible for reporting any suspected misuse or problem to the Headteacher or Head of Education for investigation, action or sanction. *(See also Whistleblowing section in the Staff handbook)*
- Ensure that any sites used for teaching purposes are suitable and that pupils are guided to such sites and that processes are in place to deal with any unsuitable material that might be located inadvertently.
- Must ensure that they do not breech copyright regulations and avoid plagiarism
- Must only use digital communication with pupils on a professional level.

2.2.4 Designated Person for Child Protection

- Must have accessed training in e-safety and be aware of serious child protection issues to arise from
  - ➢ Sharing of data
  - ➢ Access to illegal/inappropriate materials
  - ➢ Inappropriate on-line contact with adults/strangers
  - ➢ Potential and actual incidents of grooming
  - ➢ Cyber –bullying.

2.2.5 Pupils

- Are responsible for using ICT systems in accordance with the pupil Acceptable Use Policy (AUP), which they will be expected to sign before being given access to school systems
- Uphold copyright rules and avoid plagiarism
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking of images and on cyber bullying
- Should also understand the importance of adopting good e-safety practice when using digital technologies outside of school and that their actions relate to out of school activities.

2.2.6 Parents and Carers

- Will understand the pupil acceptable user policy

2.2.7   Curriculum

2.2.7.1 E-safety will be a focus within the school curriculum and staff should re-enforce safety messages across the curriculum

- In lessons where internet use is pre-planned, it is best practice that pupils be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics such as safe sex, drugs, race, discrimination that would normally result in internet sites being blocked. In such a situation, staff can request that some sites may be unblocked. This will be time limited.
- Pupils will be taught the importance of acknowledging sources.

2.3   Use of Digital and video images, photographic, video.

2.3.1   When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites (This will be part of the **CEOPS Thinkuknow** training).

- Staff may use digital and video images that but must not share, distribute or publish those images without express consent from the Head of Education. Such images should only be taken on Five Rivers equipment.
- Care must be taken that pupils are appropriately dressed if taking part in photographic exercises.
- Pupils must not share, distribute or publish images of others without the consent of both the third party and the Headteacher.
- Good practice (and good taste) will be adopted when selecting any images of pupils or staff to be used on a website or elsewhere
- Pupils' full names will NOT be used on a website or blog, particularly in association with photographs
- Written permission will be sought from parents/ carers/ or placing authorities prior to using identifiable images of children
- Pupil's work can only be published with the permission of the pupil.

2.4   Pupil Acceptable Use Agreement September 2016

2.4.1   I understand that I must use our school's ICT system in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems or other users.

2.4.2   For My Own Safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I will treat my user name like my tooth brush: I will not share it nor will I try to use any other person's user name or password
- I will be aware of 'stranger danger' when I communicate on line
- I will not disclose or share personal information about myself or others when on line
- If I arrange to meet people off line that I have communicated with on line, I will inform an adult and, if appropriate to do so, arrange to meet that person in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on line.

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

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission from a member of staff to do so. I will not use the internet for digital gaming unless given permission from a member of staff to do so.
- I will not steal, disable or cause damage to school equipment, or the equipment belonging to others.

I will act as I expect others to act towards me:

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

When using the internet for research or recreation, I recognise that:

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

I understand that I am responsible for my actions, both inside and outside of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, when I am out of school, especially if the activities involve other pupils, are hurtful or nasty.
- I understand that if I fail to comply with this agreement, I will be subject to disciplinary action which may result in the loss of access to the school ICT system. In the event of illegal activities there will be involvement with the Police.

I have read and understand the above and agree to follow these guidelines when:

- ➢ I use the school ICT system
- ➢ I use my own equipment in school (if allowed to do so)
- ➢ I use my own or Five Rivers equipment out of school in a way that is related to me being a member of the school community, i.e. communicating with other pupils, etc.

Name of Pupil ………………………………………………………………………………

Signature of Pupil ………………………………………………………………………………

2.5 Staff and Volunteer Acceptable Use

2.5.1 This Acceptable Use Policy is intended to ensure:

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

Acceptable Use Policy Agreement

2.5.2 I understand that I must use the Five Rivers School ICT systems in a responsible and acceptable way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT. I will, where possible educate the young people within my care in the safe use of ICT. I will embed e-safety in my work with young people.

For my personal and professional safety:

- I understand that
- the school will monitor my use of ICT systems, emails and other digital communications
- I understand that the rules set out in this agreement also apply to the use of school ICT systems (e.g. laptops, emails etc.) out of school.
- I understand that the school ICT systems are primarily intended for the educational use and that I will only use the systems for personal and recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else nor will I try to use any other person's password or username.
- I will immediately report any illegal, inappropriate or harmful material or incident that I become award of to the appropriate person (see the flow diagram).

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

- I will not access, copy, remove or otherwise alter another user's work or files without their express consent
- I will always communicate appropriately and professionally at all times
- I will ensure that I will uphold copyright rules and will not plagiarise other people's work
- I will always acknowledge sources
- I will ensure that whenever I take or publish images of children I shall do so using Five Rivers equipment and only after having gained permission from my line manager that this is appropriate to do.
- I shall only use chat and social networking sites in school in accordance with the school policy
- I will only communicate with pupils, parents, carers and other professionals in a professional capacity and I shall only do so using Five River's equipment.
- I will not give pupils my personal or professional email address, telephone number or provide them access to any personal social sites that I might be party to.
- I will not engage in any on-line activity that might compromise my professional responsibilities

- I will not upload or download any material which are deemed to be obscene or illegal (i.e. child sexual abuse images, criminality racist material, adult pornography) or any other material that may cause harm
- I shall not alter settings, install programmes or store information which may breech the security of the schools ICT system

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

- I understand that this Acceptable Use Policy applies not only to my work and use of School ICT equipment in school but also applies to my use of school ICT equipment out of school or in any other situation relating to my employment.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to a disciplinary action. This could include a warning, a suspension, a referral to the CEO and in some cases involvement of the Police

---

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

Name of staff or volunteer ……………………………………………………………………………….

Signed ……………………………………………………………………………….

Responding to incidents of misuse

Have you found inappropriate or illegal material on a PC?

No →

Do you suspect that inappropriate or illegal material is being accessed?

YES

YES ↓

Disconnect the computer from the mains immediately DO **NOT SHUT DOWN** (this could erase info)

Do you know when such material might have been accessed (approximate time?)

↓

Contact the Head of Operation

↓

Head of Operation will request a written report with dates and times (approx.)

↓

Do you believe that the material is illegal?

NO →

Do you have sufficient information to deal with this situation?

ICT manager will be requested to produce log file information for relevant times

No

YES

↓

Do the log files contain inappropriate/illegal materials?

YES

Inform CEO

Inform CEO

Contact the Local Police