Online Safety Policy

Safeguarding pupils, staff and school in a digital world.

This Online Safety policy recognises our commitment to e-safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe in the 'Every Child Matters' agenda.

We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to online safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets.

For the purposes of clarity and consistency throughout this document the person in school who is taking a lead on online safety is called the online safety coordinator**.**

The person in school taking on the role of online safety coordinator is Mrs Claire Lawrence.

The following groups were consulted during the creation of this Online Safety policy:

- **Directors**
- **Senior Management Team**
- **ICT Co-ordinator**
- **Teachers**

The following local and national guidance are acknowledged and included as part of our Online Safety policy:

1. Kirklees LCSB Guidance

The Kirklees Safeguarding Children's Board Procedures and Guidance
Kirklees Safeguarding procedures will be followed where an eSafety issue occurs which gives rise to any concerns related to Child Protection. In particular we acknowledge the specific guidance in:

Section 5.1.6 Child Abuse and Information Communication Technology
This section of the Kirklees Safeguarding procedures covers awareness of, and response to, issues related to child abuse and the Internet. In particular we note and will follow the advice given in the following section:

Section 7. Actions to be taken where an Employee has Concerns about a Colleague
This provides guidance on the action to be taken if an employee has either information or reason to suspect that a colleague is accessing indecent images of children.

2. DCSF Guidance

Guidance for Safer Working Practices for Adults who work with Children and Young People DCSF Jan 2009
This guidance provides clear advice on appropriate and safe behaviours for all adults working with children in paid or unpaid capacities, in all settings and in all contexts. We acknowledge the guidance given in the following sections and accept this as part of our policy. (See extract in Appendix)

- **Section 12 Communication with Children and Young People**
- **Section 27 Photography and Videos**
- **Section 28 Access to inappropriate images and Internet Usage**

3. Kirklees Guidance

The following Kirklees Guidance documents are included as part of this Online Safety policy:

Kirklees First Response Guidance for Staff (posters)

Responsibilities of the School Community

We believe that Online Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Directors accept the following responsibilities:

- Ensure adequate technical support is in place to maintain a secure ICT system.

.• Ensure procedures are in place to ensure the integrity of the school's information and data assets.

- Read, understand, contribute to and help promote the school's Online Safety policies and guidance as part of the schools entire safeguarding procedures

- Ensure appropriate funding and resources are available for the school to implement the Online Safety strategy

The Senior Management Team accepts the following responsibilities:

- Identify a person (the Online Safety coordinator- Mrs C Lawrence) to take responsibility for Online Safety and support them in their work

.• Ensure policies are in place to ensure the integrity of the school's information and data assets

- Develop and promote an Online Safety culture within the school community

- Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have Online Safety included as part of their induction procedures

- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to Online Safety

- Receive and regularly review Online Safety incident logs; ensure that the correct procedures are followed should an Online Safety incident occur in school and review incidents to see if further action is required

- Take ultimate responsibility for the Online Safety of the school community

Responsibilities of the Online Safety Coordinator

- Promote an awareness and commitment to Online Safety throughout the school

- Be the first point of contact in school on all Online Safety matters

- Create and maintain Online Safety policies and procedures

- Develop an understanding of current Online Safety issues, guidance and appropriate legislation

- Ensure delivery of an appropriate level of training in Online Safety issues

- Ensure that Online Safety education is embedded across the curriculum

- Ensure that Online Safety is promoted to parents and carers

- Ensure that any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy

- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate

- Monitor and report on Online Safety issues to the Senior Management Team and the Directors as appropriate and at the request of the Senior Management Team conduct occasional checks on files, folders, email and other digital content to ensure the Acceptable Use Policy is being followed

- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable

- Ensure an Online Safety incident log is kept up-to-date

- Ensure that Good Practice Guides for Online Safety are displayed in classrooms and around the school

Responsibilities of all Staff

- Read, understand and help promote the school's Online Safety policies and guidance

- Read, understand and adhere to the staff AUP (Acceptable Use Policy)

- Take responsibility for ensuring the safety of sensitive school data and information

- Develop and maintain an awareness of current Online Safety issues and legislation and guidance relevant to their work

- Maintain a professional level of conduct in their personal use of technology at all times

- Embed Online Safety messages in learning activities where appropriate

- Supervise pupils carefully when engaged in learning activities involving technology

- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable

- Report all Online Safety incidents which occur in the Online Safety incident log and to the Online Safety Officer

- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance

- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school

- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all Online Safety incidents to appropriate members of staff
- Discuss Online Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting Online Safety
- Read, understand and promote the pupil AUP with their children
- Discuss Online Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Acceptable Use Policies

School have separate AUP policies for pupils and staff.
These are shared with all users yearly and staff and pupils will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to school who use our ICT facilities are made aware of the appropriate AUP.

Learning and Teaching

We believe that the key to developing safe and responsible behaviour online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We will deliver a planned and progressive scheme of work to teach Online Safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity.

We believe that learning about Online Safety should be embedded across the curriculum and also taught in specific lessons in ICT and PSHE. We will discuss, remind or raise relevant Online Safety messages with pupils routinely wherever suitable opportunities arise.

We will remind pupils about their responsibilities to which they have agreed through the AUP. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through the school weekly newsletter and website.

We will ask all parents to discuss the pupil's AUP with their child and return a signed copy to the school.

We request our parents to support the school in applying the Online Safety policy.

Managing and safeguarding ICT Systems

The school will ensure that access to the school ICT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

Any administrator or master passwords for school ICT systems are kept secure and available to at least two members of staff, e.g. head teacher and a director.

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named individuals e.g. a director. We do not allow anyone except a director to download and install software onto the network.

Filtering Internet access

Web filtering of internet content is provided by Smoothwall.
This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. Notices are posted in classrooms and around school as a reminder.

Access
The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords.

All users are provided with a log in appropriate to their key stage or role in school.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users.

Using the Internet

We provide the internet to

- Support curriculum development in all subjects

- Support the professional work of staff as an essential professional tool

- Enhance the school's management information and business administration systems

- Enable electronic communication and the exchange of curriculum and administration data with the LA and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using, the school ICT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school ICT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using email

Email is regarded as an essential means of communication and the school provides all teaching staff with an e-mail account for school based communication.

Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

Use of the school e-mail system is monitored and checked.

As part of the curriculum pupils are taught about safe and appropriate use of email.

Publishing content online

e.g. using the School website, blogs, wikis, podcasts, social network sites ie school facebook page

School website:

The school maintains editorial responsibility for the school web site content to ensure that content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web site and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Online material published outside the school :

Material published by pupils and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

Using mobile phones

Please refer to separate policy attached to our Safeguarding Policy.

Using other technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an Online Safety point of view.

We will regularly review the Online Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

Protecting school data and information

School recognises their obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

Pupils are taught about the need to protect their own personal data as part of their Online Safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following :-

- Staff will be provided with encrypted USB memory sticks for carrying sensitive data
- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the schools management information systems holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on
- computers outside school
- When the directors dispose of old computers and other equipment they take due regard for destroying information which may be held on them
- Remote access to computers is by authorised personnel only
- We have some back up and recovery procedures in place for school data
- Where sensitive staff or pupil data is shared with other agencies who have a right to see the information, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

Dealing with Online Safety incidents

All Online Safety incidents are recorded in the School Online Safety Incident Log which is regularly reviewed.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious Online Safety incident, concerning pupils or staff, they will inform the Online Safety coordinator, a member of the senior management team or head teacher who will then respond in the most appropriate manner. [See **First Response Guidance to Online Safety Incidents]**

Instances of **cyberbullying** will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Online Safety coordinator and Senior Management Team and advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserve the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Kirklees Safeguarding Procedures and Guidance will be followed.
Section 5.1.6 Child Abuse and Information Communication Technology

Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitutes behaviour which we would always consider unacceptable (and possible illegal) :

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act, revised 1988

Appendix

Extract from :

Guidance for Safer Working Practice for Adults who work with Children and Young People. DCSF January 2009

Section 12 Communication with Children and Young People *(including the Use of Technology)*

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming .They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Internal e-mail systems should only be used in accordance with the organisation's policy.

This means that the organisation should:
have a communication policy which specifies acceptable and permissible modes of communication

This means that adults should:

- *not give their personal contact details to children or young people, including their mobile telephone number and details of any blogs or personal websites*
- *only use equipment e.g. mobile phones, provided by organisation to communicate with children, making sure that parents have given permission for this form of communication to be used*
- *only make contact with children for professional reasons and in accordance with any organisation policy*
- *recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible*
- *not use internet or web-based communication channels to send personal messages to a child/young person*
- *ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at maximum*

Section 27 Photography and Videos

Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet. There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them.

Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.

It is not appropriate for adults to take photographs of children for their personal use.

This means that adults should:

- *be clear about the purpose of the activity and about what will happen to the images when the activity is concluded*
- *be able to justify images of children in their possession*
- *avoid making images in one to one situations or which show a single child with no surrounding context*
- *ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed.*
- *only use equipment provided or authorised by the organisation*
- *report any concerns about any inappropriate or intrusive photographs found*
- *always ensure they have parental permission to take and/or display photographs*

This means that adults should not:

- *display or distribute images of children unless they have consent to do so from parents/carers*
- *use images which may cause distress*
- *use mobile telephones to take images of children*
- *take images 'in secret', or taking images in situations that may be construed as being secretive.*

Section 28 Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal.

This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Adults should not use equipment belonging to their organisation to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Organisations and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

This means that organisations should

- *have clear online safety policies in place about access to and use of the internet*
- *make guidance available to both adults and children and young people about appropriate usage.*
-

This means that adults should:

- *follow their organisation's guidance on the use of IT equipment*
- *ensure that children are not exposed to unsuitable material on the internet*
- *ensure that any films or material shown to children and young people are age appropriate*

Reviewed: September 2018