Online Safety (eSafeguarding) Policy

Safeguarding pupils, staff and school in a digital world

Developed by: Suzy Mattock – Assistant Headteacher

Approved by: Governors and Senior Leadership Team

Responsible Governor:

Responsible Officer:

Table of Contents

Introduction

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 of 'Keeping Children Safe in Education' 2016 and 'Working together to Safeguard Children' 2015.

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.

The internet and other digital technologies have an important role in teaching and learning, and when used safely and correctly, can bring many benefits. Technology rapidly changes and improves and we believe it is important to balance these benefits with an awareness of the potential risks. This policy has been designed to raise awareness of these risks and to highlight the school's commitment to safeguarding the wellbeing of our students.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm (DfE Keeping Children Safe in Education 2016)

This policy is to be read in conjunction with the school's Safeguarding Policy, Acceptable Use Policy and the Behavior Policy.

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. We have adopted the good practice requirements for all staff which are included in the Kirklees Information Security Guidance document.

The scope of this policy:

- This policy applies to the whole school community including the Senior Leadership Team (SLT), Governing Body (GB), all staff employed directly or indirectly by the school, visitors and all pupils.
- The Senior Leadership Team and school governors will ensure that any relevant or new legislation that may impact upon the provision for online safety within school will be reflected within this policy.

- The Education and Inspections Act 2006 empowers head teachers, to such 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 online bullying, or other online safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any material that could be used to bully or harass others.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of school.

n.b. 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 at the High School is Suzy Mattock/Sam Diskin.

The person in Netherhall St James Infant School taking on the role of Online Safety lead is Michaela Hainsworth.

The person in Netherhall Junior School taking on the role of Online Safety lead is Michaela Hainsworth.
(Both responsible to the Co.Headteachers and designated Safeguarding Lead Persons)

The Governor with an overview of Online Safety matters is Patrice Curtis

The following groups were consulted during the creation of this Online Safety policy: NLC Campus Governing Body, NLC Campus ICT Technical Team

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

1. Kirklees LSCB Guidance

The Kirklees Safeguarding Children's Board Procedures and Guidance

Kirklees Safeguarding procedures will be followed where an online safety issue occurs which gives rise to any concerns related to child protection. In particular we acknowledge the specific guidance in:

Section 1.4.6 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. Government Guidance

Keeping Children Safe in Education (DfE 2016) with particular reference to Annex C Online Safety

The Prevent Duty: for schools and childcare providers (DfE 2015)

Revised Prevent Duty Guidance for England and Wales (Home Office 2015)

How social media is used to encourage travel to Syria and Iraq - Briefing note for schools (DfE 2015)

Cyberbullying: Advice for Headteachers and School Staff (DfE 2014)

Advice on Child Internet Safety 1.0 Universal Guidelines for Providers (DfE and UKSIC 2012)

This guidance provides clear advice on appropriate and safe behaviors for all adults working with children in paid or unpaid capacities, in all settings and in all contexts.

3. Kirklees Learning Service Guidance

The following Kirklees guidance documents are included as part of this Online Safety Policy:

Kirklees Electronic Communications Guidance for School Staff

Kirklees First Responders Guidance for School Staff

The following document is included for information

Misuse of Electronic Communications – information for all Kirklees staff

All of the above policies are available on One Hub .

4. Other Guidance

Appropriate Filtering for Education Settings (UK Safer Internet Centre 2016)

Appropriate Monitoring for Schools (UK Safer Internet Centre 2016)

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 Scope of this Policy:

- To put practices into place that will safeguard and protect the students and staff at Netherhall Learning Campus.
- To assist staff and students to work safely and responsibly with the internet and other communication technologies.
- To set clear expectations of behavior and practice relevant to responsible use of the internet for educational, personal or recreational use.
- To have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other polices.
- To ensure all members of the school community are aware that unlawful or unsafe behavior is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimize the risk of misplaced or malicious allegations made against adults who work with students.

The Management Team accepts the following responsibilities:

- The Principal/Vice Principal will take ultimate responsibility for the online safety of the school community
- Identify a person (the online safety coordinator) (or team) to take responsibility for online safety and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the Governors
- 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
- Online safety will be taught as part of the curriculum in an age-appropriate way to all pupils.

Responsibilities of the online safety Coordinator

- Promote an awareness and commitment to online safety throughout the school through a targeted plan of assemblies, tutor activities and through lessons across the school community.
- Ensure all students will be taught about the impact of cyberbullying, sexting, radicalisation and trolling and know how to seek help if they are affected by any form of online bullying.
- Be the first point of contact in school on all online safety matters, ensuring all students are aware of where to seek help if they experience problems when using the internet and related technologies i.e parent/carer, teacher or trusted staff member, an orgnaistation such as Childline, CEOP.
- Lead the school online safety team
- 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 for all members of the school community
- Ensure that online safety education is embedded across the curriculum and review with regular online safety audits
- Ensure that online safety is promoted to parents and carers with all current practices and procedures in place, along with support and appropriate guidance
- 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 (KSCB) and other relevant agencies as appropriate
- Monitor and report on online safety issues to the online safety group, the Management team and Governors as appropriate
- 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
- To promote the positive use of modern technologies and the internet
- To ensure that the school Online Safety Policy and Acceptable Use Policies are reviewed at prearranged time intervals.

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
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with pupils is on a professional level and only through school based systems, NEVER through personal email, text, mobile phone social network or other online medium
- 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 appropriate log and/or to their line manager
- Respect, and share with pupils the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Additional Responsibilities of Technical Staff

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and malicious attack
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any online safety-related issues that come to their attention to the online safety coordinator and/or leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment
- Liaise with the Local Authority and others on e-safety issues
- Document all technical procedures and review them for accuracy at appropriate intervals
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance
- Take responsibility for their own and each other's' 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
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices

- To know, understand and follow school policies regarding online bullying
- 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
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images of pupils
- To agree to and sign the home-school agreement containing a statement regarding their personal use of social networks in relation the school :
  We will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's online safety policies and guidance as part of the schools overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- Ensure appropriate funding and resources are available for the school to implement their online safety strategy
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data

Responsibilities of the Designated Safeguarding Lead

- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, online bullying, radicalisation and others.
- Attend regular training and updates on online safety issues. Stay up to date through use of online communities, social media and relevant websites/newsletters.

- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.

- Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to online safety ensuring that staff know the correct child protection procedures to follow.

Responsibility of any external users of the school systems e.g. adult or community education groups; breakfast or afterschool club

- Take responsibility for liaising with the school on appropriate use of the school's ICT equipment and internet
- Ensure that participants follow agreed Acceptable Use Procedures

Acceptable Use Policies

School have a number of AUPs for different groups of users.

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.

Staff Training

Our staff will receive regular information and training on safeguarding issues. In addition, as part of the induction process, all new staff (including ITT/GTP/PGCE/SCIIT students) will receive information and guidance on our online safety policy and the school's acceptable use policy. Staff will also have regular updates around any new or developed online safety legislation or guidance produced.

All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of safeguarding and know what to do in the event of misuse of technology by any member of the school community.

Teaching and Learning

We believe that the key to developing safe and responsible behavior 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, and we believe we have a duty to prepare our students to safely benefit from the opportunities the internet brings.

- We will promote safeguarding, inclusive of online safety, through a planned programme of assemblies and whole school activities.
- 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 such as in Computing and PSCHE.
- We will discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise.
- Staff will model safe and responsible behavior in their own use of technology during lessons.
- Students will be taught the impact of cyberbullying, sexting, trolling and online threats such as radicalization and know how to seek help if they are affected by any form of online bullying threatening behavior or intimidation.
- Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.
- All teachers will ensure they are aware of their responsibilities of safeguarding online activities by completing an audit of all aspects of their curriculum.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

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 meetings, the school newsletter, website and regular updates through our online safety coordinator. .

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.

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 member of technical support.

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 member of technical support.

We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

Filtering Internet access

Web filtering of internet content is provided by NLC in conjunction with YHGfL/ICT4C 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, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

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.

Detailed guidance on the protection of sensitive school data and information assets is included in the **Kirklees Information Security Guidance** which forms part of this policy.

Password Security

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Users are provided with an individual network, email and online resources log-in username . (EY pupils are an exception to this).
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Headteacher
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS system and/or online resources, 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.
- Due consideration should be given when logging into the Virtual Learning Platform to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of the Headteacher and all staff and pupils are expected to comply with the policies at all times.
- The school maintains a log of all accesses by users and of their activities while using the system in order to track any online safety incidents.

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, the examination boards 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.

n.b. Additional guidance for staff is included in the **Kirklees Electronic Communications Guidance for Staff** and this is included as part of the school's online safety Policy.

Using email

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

- Staff and students may only use school provided email accounts for school purposes and are not permitted to access personal email accounts during school hours.
- Staff should only use school email accounts for school related business. Under no circumstances should staff contact students, parents or conduct any school business using personal email accounts.
- Communication between staff and students should be professional and related to school matters only.
- Students and staff are expected to send polite and responsible messages.
- Students and staff are made aware of the dangers of opening email from an unknown sender or source or viewing email attachments.
- All email users should report and inappropriate or offensive emails to a member of the Leadership Team through the schools incident reporting mechanism.
- Irrespective of how staff and students access their school email (from home or from school), school policies still apply.
- Use of the school e-mail system is monitored and checked

Publishing content online

E.g. using the school website, Learning Platform, blogs, wikis, podcasts, social network sites

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

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

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, e.g. divorce of parents, custody issues, etc.

Parents/ 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.

Creating online content as part of the curriculum:

As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behavior in the creation and publishing of online content. They are taught to publish for a wide range of audiences, which might include governors, parents or younger children. Personal publishing of online content is taught via age-appropriate sites that are suitable for educational purposes. They are moderated by the school where possible. Pupils will only be allowed to post or create content on sites where members of the public have access when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the school:

Staff and pupils are encouraged to adopt similar safe and responsible behaviors in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors 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.

N.B. Additional guidance for staff is included in the **Kirklees Electronic Communications Guidance for Staff** and this is included as part of the school's online safety Policy.

Using images, video and sound

We recognize 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 behavior when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; 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 (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

We secure additional parental consent specifically for the publication of pupils' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly on the website.

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.

We are happy for parents to take photographs at school events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites.

N.B. Additional guidance for staff is included in the **Kirklees Electronic Communications Guidance for Staff** and this is included as part of the school's online safety Policy.

Using video conferencing, web cameras and other online meetings

We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. We ensure that staff and pupils take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Pupils do not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

For their own protection a video conference or other online meeting between a member of staff and pupil(s) which takes place outside school or whilst the member of staff is alone is always conducted with the prior knowledge of the head teacher or line manager and respective parents and carers.

N. B. Additional guidance for staff is included in the **Kirklees Electronic Communications Guidance for Staff** and this is included as part of the school's online safety Policy

Misuse and Infringements

Complaints

Complaints relating to online safety should be made to the online safety co-ordinator or Headteacher. Incidents should be logged on.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the online safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Headteacher.

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' online safety rules. However, staffs are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

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

Using mobile phones

Student use of mobile phones:

- Mobile phones and or personal devices will not be used in any way during the lessons or formal school time. They should be switched off or stitched to silent mode.
- Mobile phones and or personal devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones.

- No images should be taken on mobile phones without the prior consent of the person or people concerned.

Staff use of mobile phones and personal devices:

- Mobile phones and or personal devices will not be used in any way during the lessons or formal school time. They should be switched off or stitched to silent mode.
- Bluetooth communication should be hidden or switched off.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students. They must only use the work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in the case of an emergency during an off-site activity, or for contacting students or parents, then a school mobile phone will be provided. In an emergency where a staff member doesn't have access to a school owned device, then they should sue their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Unauthorised publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter.

Using mobile devices

We recognize that the multimedia and communication facilities provided by mobile devices (e.g. iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities for pupils. However their use in lesson time will be with permission from the teacher and within clearly defined boundaries.

Pupils are taught to use them responsibly.

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. The online safety policy will be reviewed annually.

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

The school is a registered Data Controller under the Data Protection Act 1998 and we comply at all times with the requirements of that registration.

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.

Staff are made fully aware of the contents of the **Kirklees Information Security Guidance for Staff** which is included as part of this policy.

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

- Staff are 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 we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- We follow Kirklees procedures for transmitting data securely and sensitive data is not sent via emailed unless encrypted
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for school data
- All devices taken off site, e.g. laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.

Management of assets

Details of all school-owned hardware and software are recorded in an inventory.

Disposal of electronic waste is the responsibility of the Campus ICT Technical Manager, based at the High School. All redundant IT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data; there is a full audit trail with descriptions, serial numbers and asset tag numbers; and certified physical destruction of hard drives.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

In addition to this, any hard drives from servers are also put through a multi-pass data erasure program on campus prior to physical destruction by contractors. The multi-pass erasure program approaches US DoD standards.

If hard drives are exchanged under manufacturer's warranty we would require a commitment to physical destruction from the manufacturer, before the drives leave site.

WEEE Waste Transfer Notes and associated documentation are retained at the High School.

Dealing with online safety incidents

All online safety incidents are recorded in the School online safety 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, their line manager or head teacher who will then respond in the most appropriate manner.

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 technical support and appropriate 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 and search any technology equipment on the premises, including personal equipment, including when a breach of this policy is suspected.

Dealing with a Safeguarding issue arising from the use of technology:

If an incident occurs which raises concerns about Safeguarding or the discovery of indecent images on the computer, then the procedures outlined in the Kirklees Safeguarding Procedures and Guidance will be followed, see also Safeguarding policy.

Section 1.4.6 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 behavior 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, extremist 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:

- 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

The following activities would normally be unacceptable; however in some circumstances they may be allowed e.g. as part of planned curriculum activity or as system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another persona to log in using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Guidance for staff on the consequences of the misuse of electronic equipment can be found in the document **'Misuse of electronic communications by staff'**

Further resources

There is a comprehensive online safety section available from the YHGfL website www.yhgfl.net

- **Acceptable Use Policies (Pupils, Staff, Temporary and Supply staff and Visitors, Community users)**
- **Letter for Parents explaining the AUP and agreement to sign**
- **Kirklees Electronic Communications Guidance for Staff**
- **Kirklees Information Security Guidance for Staff**
- **Kirklees First Responders Guide to online safety incidents**
- **Kirklees Misuse of Electronic Communications by Staff**
- **Practical Guidance for protecting school information**

- **Guidance for using children's images and voices in publications and on web sites**