Castle Hill School

Online Safety Policy

Updated July 2018

Policy Created	2016
Committee	Gov Body
Signed off **Last review**	2018
Review frequency	Biennial
Date to be reviewed	2020

Castle Hill School

Kirklees COUNCIL

Table of Contents

Castle Hill School

Kirklees COUNCIL

Acknowledgement

This policy is based on an original document '**YHGfL Guidance for Creating an eSafety Policy**' written by Yorkshire and Humberside Grid for Learning. It has been adapted and updated by Kirklees Learning Service for use in Kirklees Schools.

1.Introduction

This Online Safety policy recognises the commitment of our school to keeping staff and pupils safe online and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. 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. 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 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. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

Our expectations for responsible and appropriate conduct are set out 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 from loss or inappropriate use.

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 Principal 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.

The person in school taking on the role of Online Safety lead is Greg Firth

The Governor with an overview of Online Safety matters is Kate Shepherd

This Online Safety policy was created by Kirklees Council, Greg Firth (ICT Manager), Alison Ley (Deputy Principal)

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

The policy was completed on: 4th May 2018

The policy was approved by Local Governing Body on 10th July 2018

The policy is due for review no later than: 3rd May 2020

Implementation of the policy

- The Senior Leadership Team will ensure all members of school staff are aware of the contents of the school Online Safety Policy and the use of any new technology within school.
- All staff, pupils, occasional and external users of our school ICT equipment will sign the relevant Acceptable Use Policies
- All amendments will be published and awareness sessions will be held for all members of the school community.
- Online safety will be taught as part of the curriculum in an age-appropriate way to all pupils.
- Online safety posters will be prominently displayed around the school.
- The Online Safety Policy will be made available to parents, carers and others via the school website or VLE.

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 Principals and School Staff (DfE 2014)

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

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)

2. 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 senior leadership team accepts the following responsibilities:

- The Principal will take ultimate responsibility for the online safety of the school community
- Identify a person (the Online Safety Lead) to take day to day responsibility for online safety; provide them with training; monitor 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, pupils and other users 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

Responsibilities of the Online Safety Lead

- Promote an awareness and commitment to online safety throughout the school
- Be the first point of contact in school on all online safety matters
- Take day to day responsibility for online safety within the school
- Lead the school online safety team and/or liaise with technical staff on online safety issues
- Create and maintain online safety policies and procedures
- Develop an understanding of current online safety issues, guidance and appropriate legislation through regular training
- 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 online safety group, the Leadership team and the Safeguarding/Online Safety Governor as appropriate

- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident
- 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, including filtering and monitoring, are in place to safeguard the security of the school IT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and detection and prevention of malicious attack
- At the request of the Leadership Team conduct periodic checks on files, folders, email, internet use 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 Lead and/or Senior 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, including password management
- Ensure that suitable access arrangements are in place for any external users of the schools IT equipment
- Liaise with the Local Authority, internet providers and others as necessary on online 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 (where possible and appropriate)

- Read, understand and adhere to the pupil AUP (child parent responsible use of internet) 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
- 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

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 child parent responsible use of internet which clearly sets out the use of photographic and video images of pupils
- To agree to and sign the child parent responsible use of internet containing a statement regarding their personal use of social networks in relation the school :

  As Parents 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 the Local Governing Body

- Read, understand, contribute to and promote the school's online safety policies and guidance as part of the school's 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
- 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
- Ensure appropriate funding and resources are available for the school to implement the online safety strategy

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 after school club

- Take responsibility for liaising with the school on appropriate use of the school's IT equipment and internet, including providing an appropriate level of supervision where required
- Ensure that participants follow agreed Acceptable Use Procedures

3. Acceptable Use Policies

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

These are shared with all users yearly and staff and pupils (where possible and appropriate) 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.

School Acceptable Use Policy documents

Staff Visitor Acceptable Use Policy (Staff, Supply Staff, Visitors, Community Users, Local Governors, Directors and Members)

Pupil AUP – Child Parent Responsible use of the internet (Letter sent for parental agreement)

Student Permissions Form (clearly defining the use of student images)

4. Training

Technology use changes at a fast pace, and we recognise the importance of regular staff training. The Online Safety Lead will attend training updates at least once per year. All school staff will receive regular updates on risks to pupils online from the Online Safety Lead, and attend online or external training as necessary.

5. Learning and Teaching

We believe that the key to developing safe and responsible behaviors 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 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. Online safety is taught in specific Computing and PSHE lessons and also embedded across the curriculum, with pupils being given regular opportunities to apply their skills.

We teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind pupils about the responsibilities to which they have agreed through the AUP.

Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

6.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 and website.

We will ask all parents to discuss the pupil's AUP with their child where possible and appropriate and return a signed copy to the school. . This includes a statement about their use of social networks in situations where it could reflect on our school's reputation and on individuals within the school community.

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

7.Managing and Safeguarding IT systems

The school will ensure that access to the school IT 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.

All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. Principal 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

In order to be compliant with the Prevent Duty and Safeguarding Children in Education 2016, the school will:

- As part of the Prevent duty, carry out an annual assessment of the risk to pupils of exposure to extremist content in school
- Ensure that all reasonable precautions are taken to prevent access to illegal and extremist content. Web filtering of internet content is provided by Kirklees Council and an onsite Smoothwall appliance; the provider is an IWF member and blocks access to illegal child abuse images and content. The provider filters the police assessed list of unlawful terrorist content produced on behalf of the home office. The school is satisfied that web filtering manages most inappropriate content including extremism, discrimination, substance abuse, pornography, piracy, copyright theft, self-harm and violence. However it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own internet activity.
- Inform all users about the action they should take if inappropriate material is accessed or discovered on a computer. Deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

- Expect teachers to check websites they wish to use prior to lessons to assess the suitability of content.
- Post notices in classrooms and around school as a reminder of how to seek help.

Monitoring

In order to be compliant with the Prevent Duty and Safeguarding Children in Education 2016, the school will:

- Use the findings of the annual Prevent risk assessment to put appropriate internet and network monitoring systems in place.
- Pupils are always supervised by staff while using the internet as this reduces the risk of exposure to extremist, illegal or inappropriate material; direct supervision also enables school staff to take swift action should such material be accessed either accidentally or deliberately.

Access to school systems

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.

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.

Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).

- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.

- All classes have a unique, individually-named user account and password for access to IT equipment and information systems available within school.

- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.

- 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.

8. Using the internet

We provide the internet to

- Support teaching, learning and 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 behavior whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school IT 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. 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. Email 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. There are systems in place for storing relevant electronic communications which take place between school and parents.

Use of the school email system is monitored and checked.

It is the personal responsibility of the email account holder to keep their password secure.

As part of the curriculum, where appropriate, pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

School will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils on the out-of-school times when emails may be answered.

Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses.

Responsible use of personal web mail accounts on school systems is permitted outside teaching hours or for non-teaching staff when on a lunch break.

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.

Publishing content online

E.g. using the school website, learning platform, blogs, wikis, podcasts, social network sites

School website:

The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the 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. Contact details for staff published are school provided.

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:

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, local 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 recognise that many aspects of the curriculum can be enhanced by the use of multimedia 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.

School will take photographs and videos at whole school events, these will be made available to parents. This is due to keeping in line with the Safe Guarding policy and to ensure that pupils who do not have the appropriate permissions are kept safe.

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 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.

Using mobile phones

Use of personal mobile phones is not permitted within the School.

Where required for safety reasons in off-site activities, a school mobile phone is provided for staff for contact with pupils, parents or the school. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent. (*In an emergency, where a staff member doesn't have access to a school-owned device, they should use 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, including to record voice, pictures or video is forbidden. 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. If the victim is another pupil or staff member we do not consider it a defense that the activity took place outside school hours.

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

We make it clear to staff, pupils and parents that the Principal has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

Using wearable technology

Wearable technology includes electronic fitness trackers and internet enabled 'smart' watches. Wearable technology is permitted on school but must not be used during lessons. Personal devices are brought onto school premises by staff or pupils at their own risk. The school does not accept liability for loss or damage of personal devices.

Wearable technology is not to be worn during tests or examinations.

Unauthorised or secret use of a wearable device or other electronic device, including to record voice, pictures or video is forbidden.

Using mobile devices

We recognise 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 evaluate 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, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behavior to those outlined in this document.

9.Protecting school data and information

School recognises the obligation to safeguard staff and pupils' sensitive and 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 General Data Protection Regulation 2018 (GDPR) and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.

Pupils are taught (where possible and appropriate) 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 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 school management information system 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
- 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.
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- We follow procedures for transmitting data securely and sensitive data is not sent via email unless encrypted
    - Castle Hill School makes use of Microsoft Office 365 for email and the use of the word 'secure' in the email subject will send the email using Office Message Encryption (OME) This ensures the email and attachment are delivered to the recipient in an encrypted method.
    - We refer to sensitive Data as defined by the Information Commissioners Office (ICO) as personal data – Further explanation is available on their website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
- Remote access to computers is by authorized personnel only
- We have full back up and recovery procedures in place for school data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example local governors or Kirklees officers, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

Management of assets

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

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.

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.

10. Responding to 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 Lead, their line manager or the Principal who will then respond in the most appropriate manner. [See **First Responders Guide to eSafety Incidents]**

Instances of **online bullying** will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognizes that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

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 Lead 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 reserves 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 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

- Restorative practice will be used to support the victims
- 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 constitute 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
- staff 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 plagiarizing of online content)
- transferring sensitive data insecurely or infringing the conditions of the GDPR

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a 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 person 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'**