Scissett Middle School

Working together, respecting all, because everyone matters

Online Safety and ICT Policy

Signed: _____ _____

Headteacher **Chair of Governors**

Agreed: 8 July 2019

Updated: 2 October 2018

Next review date: 2 October 2020

Table of Contents

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 2018)

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 policy

- This policy applies to the whole school community including the Board of Directors, Governing Body Senior, Leadership Team, Governing Body, all staff employed directly or indirectly by the school, visitors and all pupils.
- The Board of Directors, Governors and Senior Leadership Team 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 head teacher 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 persons in school taking on the role of Online Safety lead are

Mrs N Greenough – Headteacher
Mrs G Senior – SENDCO/Designated Safeguarding Lead
Mr J Hampson – Head of Year and Strategic Lead for Attendance

The Governor with an overview of Online Safety matters is
Dr S Brown – LA Governor

This Online Safety policy was created by
Mr J Ambler – ICT Manager

The policy was approved by the Board of Governors on 8 July 2019

The policy was reviewed by
Mr J Ambler in October 2019 and is due for review in October 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.

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 2018) 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)

3. Kirklees Guidance

The following documents derived from Kirklees Council's guidance are included as part of this Online Safety Policy:

The Mast Electronic Communications Guidance for School Staff

Kirklees Council First Responders Guidance for School Staff

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 Headteacher 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

- 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 networking or other online mediums such as chat apps.

- Not to partake in online activity which is likely to adversely impact on the reputation of the school
- 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 prevention
- 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 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 school's ICT equipment
- Liaise with the Local Authority and others 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
- Access emails and files on school systems if required, belonging a member of staff who is absent due to being on holiday, illness etc

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
- Not to partake in online activity which is likely to adversely impact on the reputation of the school
- 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
- Agree to 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

- The school makes use of fingerprint readers for the purposes of loaning library books and purchasing school meals. These systems do not store a reproducible image of a child's fingerprint. If you have no objections, please opt-in to your child having their fingerprints scanned by responding to the letter regarding the use of biometrics in school sent out in Year 6

Responsibilities of Governing Body

- Read, understand, contribute to and help 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 their 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

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 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

LINKS:

Pupil
Staff
Visitor and Community Users

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.

Learning and Teaching

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

We will deliver a planned and progressive scheme of work to teach online safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. We believe that learning about online safety should be embedded across the curriculum and also taught in specific lessons such as in Computing and Citizenship.

We will 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 will 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.

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 and return a signed copy to the school.

We request that they 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.

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 and data held on the machine is encrypted.

All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. Assistant Deputy Head (Data) and members of technical support.

The wireless network is protected by a secure log on which prevents unauthorised 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 for limited periods and purposes only (e.g. to install a printer at home).

Filtering and Monitoring Internet access

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 a Smoothwall appliance and Impero Education Pro software; both providers are IWF members and block access to illegal child abuse images and content. The providers' 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.
- Internet and network use is monitored daily using both reports and real-time monitoring by the school IT Manager and Technician to identify access to websites, typed key words or internet searches which are a cause for concern. Minor infringements such use of swearwords and inappropriate language are reported to the pupil's Head of Year, serious issues such as safeguarding concerns are reported the Safeguarding Team or Headteacher.

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.

To ensure consistency, permissions on new user accounts are copied from the account of an existing user with the same role.

Where a new role is created the permissions are defined through discussion with the user's line manager and the Assistant Deputy Head (Data).

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 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.

Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system). Passwords must be at least 8 characters in length with at least 1 uppercase character and 1 number. Symbols are optional.

- 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 pupils 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.

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 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 Mast Electronic Communications Guidance for Staff** and this is included as part of the school's online safety Policy.

Using email and other means of 2-way contact

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 pupils are taught about safe and appropriate use of email and other means of 2-way communication such as social networks and online chat facilities. 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, via social media or chat systems.

Responsible use of personal web mail accounts on school systems is permitted outside teaching hours.

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

Pupil email accounts can only send and receive emails to/from approved senders.

Publishing content online

E.g. using the school website, learning platforms, 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.

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 behaviour 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 behaviours 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 **The Mast 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 multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants 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 filename 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 **The Mast 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. Video conferencing is only available to teaching staff's accounts and not pupils' to ensure that all activity is supervised. Pupils do not operate video conferencing software, answer calls or set up meetings without permission from the supervising member of staff.

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 Mast Electronic Communications Guidance for Staff** and this is included as part of the school's online safety Policy.

Using mobile phones

Use of mobile phone is covered by a separate policy.

Using wearable technology

Wearable technology includes electronic fitness trackers and internet enabled 'smart' watches. Wearable technology is permitted on school premises but must not be used during lessons. Personal devices are brought onto school premises by staff and 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.

Using mobile devices

We recognise that the multimedia and communication facilities provided by mobile devices 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 behaviour to those outlined in this document.

Protecting school data and information

School recognises their 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 Regulations (GDPR) 2018 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 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:

- Data held on staff computers is encrypted. Where staff require a USB stick, an encrypted one will be provided by IT staff. No personal or unencrypted USB sticks are to be used for school purposes.
- All computers or laptops holding sensitive information are set up with strong passwords 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 held 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 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

- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example 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 2013 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2018.

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 Lead, their line manager or the Headteacher 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 recognises 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, appropriate advice will be sought and action taken to minimise 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. Data breaches will be reported according to the duties stated in the General Data Protection Regulations (GDPR) 2018.

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 possibly 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
- partaking in online activity which is likely to adversely impact on the reputation of the school
- 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 plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the General Data Protection Regulations (GDPR) 2018

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

- ICT staff occasionally need to reset passwords to gain access to other users' accounts for troubleshooting purposes, this would always be done with the consent of the user and for more serious or long-term issues rather than as a matter of course.
- there are situations where access to users' accounts may be required via password reset with the approval of the Headteacher, e.g. if the user were under investigation, or if it was necessary to retrieve information due to a member of staff being on long term sick/out of the country/having left. This access would be logged.
- maliciously 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 'Electronic Communications Policy'

References to related documents:

- Acceptable Use Policies
  (Pupils, Staff (including temporary staff) , Visitors and Community Users)
- Letter for Parents explaining the AUP and agreement to sign
- The Mast Electronic Communications Guidance for Staff
- Kirklees Information Security Guidance for Staff
- The Mast Electronic Communication Guidance for School Staff
- Department for Education – Data Protection: Toolkit for Schools
- Guidance for using children's images in publications and on web sites

Accounts with third party organisations

Google

Scissett Middle School uses the Google G Suite for Education Suite to enhance the way we use technology and provide greater access to learning resources both inside and outside school.

Google G Suite for Education is a cloud based learning platform allowing teachers and students to create and collaborate using a wide variety of cloud based applications provided by Google, this allows

us to offer a range of new learning opportunities for teachers and pupils. Further information can be found at https://www.google.com/edu/products/productivity-tools.

Education Terms

Department for Education – Cloud (educational apps) software services and Data Protection

Access is subject to parental approval on an opt-in basis, a letter is sent out to parents of new pupils informing them of this.

Educational Websites

It is necessary to share pupil information with providers of educational websites such as TT Rockstars and Bedrock Learning. This is always done in compliance with GDPR legislation.