

# Barkisland CE (VA) Primary School

## ESafety Policy



### Table of Contents

1. Introduction
2. Responsibilities of the School Community
3. Acceptable Use Policies (AUP)
4. Learning and Teaching
5. Parents and carers
6. Managing and safeguarding ICT Systems
7. Using the Internet; email; publishing content online; using images, video & sound; using video conferencing and other online text or video meetings; using mobile phones; using other technologies
8. Protecting school data and information
9. Dealing with eSafety incidents

### Acknowledgement

This document is based on an original document 'YHGfL Guidance for creating an eSafety Policy'

### Introduction

This eSafety policy recognises the commitment of our school to eSafety 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 eSafety 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. 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 formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to eSafety 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 senior leadership team, (SLT) school board of governors, all staff employed directly or indirectly by the school, visitors and all pupils.
- The senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for eSafety 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 cyberbullying, or other eSafety-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 eSafety behaviour that take place out of school.

### **Implementation of the policy**

- The senior leadership team will ensure all members of school staff are aware of the contents of the school eSafety 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.
- eSafety will be taught as part of the curriculum in an age-appropriate way to all pupils.
- eSafety will be addressed through whole school themed weeks such as; Diversity Week and Keeping Safe Week.
- eSafety posters will be prominently displayed around the school.
- 
- The eSafety policy will be made available to parents, carers and others via the school website.

### **Responsibilities of the School Community**

We believe that eSafety 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:**

- Becky Schofield (headteacher) will take ultimate responsibility for the eSafety of the school community.
- Sarah Wilde (eSafety lead) to take day to day responsibility for eSafety; 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 eSafety culture within the school community.
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have eSafety 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 eSafety.
- Receive, and regularly review, eSafety incident logs; ensure that the correct procedures are followed should an eSafety incident occur in school and review incidents to see if further action is required.

### **Responsibilities of the eSafety Lead**

- Promote an awareness and commitment to eSafety throughout the school.
- Be the first point of contact in school on all eSafety matters.
- Take day to day responsibility for eSafety within the school.
- Lead the school eSafety team and/or liaise with technical staff on eSafety issues.
- Create and maintain eSafety policies and procedures.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure delivery of an appropriate level of training in eSafety issues.
- Ensure that eSafety education is embedded across the curriculum.
- Ensure that eSafety 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 eSafety issues to the Leadership team and the Safeguarding/eSafety 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 eSafety incident.

- Ensure an eSafety incident log is kept up-to-date and incidences are recorded on CPOMS.
- Ensure that Good Practice Guides for eSafety are displayed in classrooms and around the school.
- To promote the positive use of modern technologies and the internet.
- To ensure that the school eSafety policy and Acceptable Use Policies are reviewed at prearranged time intervals.

### **Responsibilities of all Staff**

- Read, understand and help promote the school's eSafety 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 eSafety 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 **and parents** is on a professional level and only through school based systems, **NEVER** through personal email, text, mobile phone, social networks or other online medium.
- Embed eSafety 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 eSafety incidents which occur in the appropriate log and/or to their line manager (CPOMS).
- 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 eSafety-related issues that come to their attention to the eSafety 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 ICT equipment.
- Liaise with the Local Authority and others on eSafety 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 eSafety incidents to appropriate members of staff.
- Discuss eSafety 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 Cyberbullying.

## **Responsibilities of Parents and Carers**

- Help and support the school in promoting eSafety.
- Read, understand and promote the pupil AUP with their children.
- Discuss eSafety 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 AUP agreement which clearly sets out the use of photographic and video images of pupils.
- To agree to and sign the AUP 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 eSafety 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 eSafety 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 eSafety strategy.

## **Responsibilities of the Child Protection Officer**

- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.
- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, cyberbullying, extremism, radicalisation and others.
- Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to eSafety 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 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 AUP 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.

**Barkisland Primary School**  
**Early Years Pupil Acceptable Use Agreement**

- I will take care when using the school IT equipment and use it properly
- I will only share any passwords or login details with trusted adults
- I will tell an adult if I see anything which upsets me
- I will only take a photograph or video of someone if they say it is alright
- Any messages I send will be polite
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a period of time, even if it was done outside school

Pupil name.....

Signed.....



## **Barkisland Primary School**

### **Key Stage 1 Pupil Acceptable Use Agreement**

- I will look after all the school IT equipment and use it properly
- I will only share my password or login details with trusted adults
- I will tell an adult if I see anything which upsets me
- I will always ask before downloading from the internet or using material I have brought into school because I understand the risks from virus infections
- Any work I upload to the internet will be my own
- I will only take a photograph or video of someone if they say it is alright
- All of the messages I send will be polite
- I will not send messages which upset other people
- I will not give away my personal information or talk to people I do not know using the internet
- I understand that the school may check my use of IT and talk to my parent or carer if they are worried about my eSafety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a period of time, even if it was done outside school

Pupil name.....

Signed.....

**Barkisland Primary School**  
**KS2 Pupil Acceptable Use Agreement**

*These rules will keep me safe at school and at home and help me to be fair to others.*

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible. This includes email, mobile phones and gaming sites.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

*I have read and understand these rules and agree to them.*

*Signed:*

*Date:*

## **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 eSafety 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 eSafety should be embedded across the curriculum and also taught in specific lessons such as in **Computing** and **PSHE**.

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 eSafety 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 our **X account, the school newsletter, School Spider and website**.

We ask parents to sign the AUP agreement which 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 eSafety policy.

## **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. head teacher, admin 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 **EXA???**. This ensures that all reasonable precautions are taken to prevent access to illegal content. 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.

All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

Teachers are encouraged to check out websites/ videos they wish to use prior to lessons for the suitability of content. Youtube is a wonderful resource for teaching and learning. Staff must make sure all content is appropriate before displaying, including adverts embedded within the video and to the side. Notices are posted in classrooms and around school as a reminder of how to seek help.

### **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.

Pupils are taught about safe practice in the use of their log in and passwords e.g Seesaw, MyMaths, TTRockstars

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.

Where appropriate, pupils have a unique, individually-named user account and password for access to online learning platforms such as Seesaw, MyMaths.

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 eSafety 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.

### **Using email**

Email is regarded as an essential means of communication and the school provides certain members of the school community with an e-mail account for school based communication. E-mail messages on school business should 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.

**Staff should periodically delete any emails that do not need to be stored or used as reference.**

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

Under no circumstances will staff contact pupils or parents using a personal email address. All forms of electronic communication are to go via the office email ([admin@barkisland.calderdale.sch.uk](mailto:admin@barkisland.calderdale.sch.uk))

Responsible use of personal web mail accounts on school systems is permitted outside teaching hours, although not encouraged.

### **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. 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.

### **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 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, on websites and the newspaper) and this list is checked whenever an activity is being photographed or filmed. Each class teacher has a copy in their classroom of these permissions.

Photographs of pupils may only be taken on personal mobile phones under the agreement they are for school use only and are deleted as soon as is practically possible e.g. once uploaded onto the school system or printed for school use. 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.

### **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 will always be conducted with the prior knowledge of the head teacher or line manager and respective parents and carers.

### **Using mobile phones**

Use of mobile phones by pupils is not permitted in school. During lesson time we expect all mobile phones belonging to staff to be switched off/put on silent unless there is a specific agreement for this not to be the case.

Where required, staff may use their mobile phones to contact the school. Staff will not normally use personal mobile phones where their mobile phone number or other personal details may be revealed to a pupil or parent, unless using the service 141 to hide their number.

Unauthorised or secret use of a mobile phone or other electronic device, 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 Headteacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

### **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 eSafety point of view.

We will regularly review the eSafety 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 Data Protection Act 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 eSafety 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.
- 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 School improvement 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.

### **Dealing with eSafety incidents**

All eSafety incidents are recorded on the school's CPOMS system. The Headteacher, Deputy Headteacher and **Pastoral Support Worker** are alerted to incidents as soon as they are recorded. 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 eSafety incident, concerning pupils or staff, they will inform the eSafety Lead 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, 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 eSafety Lead and technical support and appropriate advice 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. 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 Calderdale Safeguarding Procedures and Guidance will be followed.

#### **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 plagiarising of online content).
- transferring sensitive data insecurely or infringing the conditions of the Data protection Act.

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.

Reviewed September 2024