Mulgrave Primary School

Learn | Believe | Succeed

Name of Policy	Cyber Security Policy
Frequency of review	Bi-annually
Agreed Date	January 2025
Review Date	January 2027

Introduction

Cyber security has been identified as a risk for the School and every employee needs to contribute to ensure data security. The School has invested in technical cyber security measures but we also need our employees to be vigilant and to act to protect the School IT systems. Plum Innovations is responsible for cyber security within the School. If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our Data Protection Policy, Data Breach Policy, Acceptable Use Policy, Home Working Policy, Electronic Email Information and Communications Policy.

Purpose and Scope

The purpose of this document is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as to set out an action plan should the School fall victim to cyber-crime. This policy is relevant to all staff.

What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks. The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- cost;
- confidentiality and data protection;
- potential for regulatory breach;
- reputational damage; business interruption;
- structural and financial instability.

Cyber-Crime Prevention Given the seriousness of the consequences noted above, it is important for the School to take preventative measures and for staff to follow the guidance within this policy. This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime.

The School Business Manager can provide further details of other aspects of the School risk assessment process upon request.

The School have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff. Technology Solutions

The School have implemented the following technical measures to protect against cyber-crime:

(i) firewalls;

(ii) anti-virus software;

(iii) anti-spam software;

(iv) auto or real-time updates on our systems and applications;

(v) URL filtering;

(vi) secure data backup;

(vii) encryption;

(viii) deleting or disabling unused/unnecessary user accounts;

(ix) deleting or disabling unused/unnecessary software;

(x) using strong passwords;

(xi) disabling auto-run features.

Controls and Guidance for Staff

• All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.

• All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the School or any third parties with whom we share data.

• All staff must:

- Choose strong passwords (the School's IT team advises that a strong password contains list of types of characters, password length etc. as permitted by your IT systems);

- keep passwords secret;

- never reuse a password;

- never allow any other person to access the school's systems using your login details;

- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the School IT systems;

- report any security breach, suspicious activity or mistake made that may cause a cyber-security breach, to the school office as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy;

- only access work systems using computers or phones that the school owns. Staff may only connect personal devices to the public and/or visitor Wi-Fi provided;

- not install software onto your school computer or phone. All software requests should be made to Mandy Butler who will discuss any requirements with ATS;

- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks.

• The School considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against the School or using the School's systems;

- accessing inappropriate, adult or illegal content within School premises or using School equipment; - excessive personal use of School's IT systems during working hours;

- removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy;

- using School equipment in a way prohibited by this policy;

- circumventing technical cyber security measures implemented by the School's IT team;

- failing to report a mistake or cyber security breach.

Cyber-Crime Incident Management Plan The incident management plan consists of four main stages:

(i) Containment and recovery: To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost.

(ii) Assessment of the ongoing risk: To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed and any consequences of the breach/attack identified.

(iii) Notification: To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.

(iv) Evaluation and response: To evaluate future threats to data security and to consider any improvements that can be made. Where it is apparent that a cyber-security incident involves a personal data breach, the School will invoke their Data Breach Policy rather than follow out the process above.

Monitoring and Filtering

Monitoring of the ICT Systems Any unauthorised use of the School's ICT systems, cloud-based ICT systems, the internet, e-mail and/or social networking site accounts which the School Business Manager and/or Plum Innovations considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority. The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

· The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device;

· This technology may be used, however for educational purposes, as mutually agreed with the Head teacher. The device user, in this instance, must always ask the prior permission of the bill payer;

· Pupils are not allowed to bring personal mobile devices/phones to school without the permission of the class teacher and these phones should be stored in the class 'phone box' and taken to and collected from the office at the start and end of the day;

· The school is not responsible for the loss, damage or theft of any personal mobile device; 8

· Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device School provided Mobile devices (including phones)

· The sending of inappropriate text messages between any member of the school community is not allowed;

· Permission must be sought before any image or sound recordings are made on the devices of any member of the school community;

· Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used; · In cases where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct

written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

· The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed;

· Staff must use the official school e-mail system for work e-mails, ie Staff Mail;

· It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. This should be the account that is used for all school business;

· Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses;

· E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper;

· Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account;

· Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes;

· All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments;

· Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail;

· Staff must inform (the e-Safety co-ordinator and Headteacher) if they receive an offensive e-mail;

· Pupils are introduced to email as part of the Computing Scheme of Work

Safe Use of Images

Taking of Images and Film Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

· With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment;

· Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device;

· Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

Publishing pupil's images and work on a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

· on the school web site;

· in the school prospectus, newsletter and other printed publications that the school may produce for promotional purposes;

· recorded/ transmitted on a video or webcam;

· in display material that may be used in the school's communal areas;

· in display material that may be used in external areas, i.e. exhibition promoting the school;

· general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically). 10 This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Web Manager has authority to upload to the site.

Storage of Images

· Images/ films of children are stored on the school's equipment;

· Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher;

· Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network;

· images are deleted when they are no longer required, or the pupil has left the school.

Misuse and Infringements Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Acting Headteacher. Incidents should be logged.

Inappropriate material

· All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator;

· Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Acting Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart);

· Users are made aware of sanctions relating to misuse or misconduct. All staff are aware of the policy and the children have signed an acceptable use policy.

Equal Opportunities Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety.

Internet activities are planned and well managed for these children and young people. Parental Involvement We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Parents/ carers are required to make a decision as to whether they consent to images of their child being

taken/ used in the public domain (e.g. on school website) The school disseminates information to parents relating to e-Safety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website/ Learning Platform postings and
- Newsletter items
- Learning platform training
- Weekly updates from The National College

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them. This policy will be reviewed every 24 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way. Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Benjamin, the school e-Safety coordinator.

·I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

·I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

·I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

·I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.

·I will only use the approved, secure email system(s) for any school business.

·I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

·I will not install any hardware of software without permission of Mr Benjamin

·I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

·Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.

·I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

·I will respect copyright and intellectual property rights.

·I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

·I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

·I will not invite or accept a child or a parent as a 'friend' on Facebook or other social networking site. User Signature I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……

Date ……

Full Name ……(printed)

Job title . . . . . .