

Online Safety Policy

Together, we **CARE!**



"Be kind and loving to each other".

Ephesians 4:32 (ICB)

Mepal & Witcham Primary School
a part of Ely Diocese Multi Academy Trust

Approved by the Governing Body: *Joy Walker*

Signed: Mr C Snuggs

Date: 22/01/25

Date to be reviewed: Feb 2026

Contents

1. Aim
2. Roles and responsibilities
 - a. Headteacher and Senior Leaders
 - b. Governors
 - c. Designated Safety Lead
 - d. Curriculum Leads
 - e. Teaching and Support Staff
 - f. IT Provider
 - g. Learners
 - h. Parents and Carers
 - i. Professional Standards
3. Reporting and Responding
4. Technology and Security
 - a. Mobile Technologies
 - b. Personal Devices
 - c. Social Media
 - d. Digital and Video Images
5. Filtering and Monitoring
 - a. Filtering
 - b. Monitoring
6. Data Protection
7. Link with other policies
8. Appendix 1

1. Aims

This Online Safety Policy outlines the commitment of Mepal and Witcham Church of England Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

The school Online Safety Policy sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication. It allocates responsibilities for the delivery of the policy and is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours. It establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world.

This policy describes how the school will help prepare learners to be safe and responsible users of online technologies and establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms. It is supplemented by a series of related acceptable use agreements and is made available to staff at induction and through normal communication channels such as staff meetings.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Mepal and Witcham Church of England Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

2. Roles and responsibilities

The school will monitor the impact of the policy using the following:

- Logs of reported incidents
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Surveys/questionnaires of:
 - Learners
 - Parents and carers
 - Staff.

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

2a. Headteacher and Senior Leaders

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead.

The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

2b. Governors

Governors are responsible for checking and monitoring the practices outlined in the Online Safety Policy.

This review will be carried out by the Chair of Governors, whose members will receive regular information about online safety incidents and monitoring reports. The safeguarding governor will take on the role of Online Safety Governor to include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety Lead;
- Regularly receiving (collated and anonymised) reports of online safety incidents;
- Checking the provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards.
- Report to relevant governors group/meeting;
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

- The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

2c. Designated Safety Lead (DSL)

The DSL will action the following:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online;
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out;
- Attend relevant governing body meetings/groups;
- Report regularly to headteacher/senior leadership team;
- Working with the Headteacher in handling incidents, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety);
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments;
- Have a leading role in establishing and reviewing the school online safety policies/documents;
- Promote an awareness of and commitment to online safety education/ awareness raising across the school and beyond;
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents;
- Provide (or identify sources of) training and advice for staff/ governors/ parents/carers/ learners;
- Liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant);
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined in Keeping Children Safe in Education:
 - Content
 - Contact
 - Conduct
 - commerce

2d. Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

This will be provided through:

- PSHE and SRE programmes.
- A mapped cross-curricular programme.
- Assemblies and pastoral programmes.
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

2e. Teaching and Support Staff

School staff are responsible for ensuring that they adhere and action the following:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices;
- They understand that online safety is a core part of safeguarding;
- They have read, understood the staff acceptable use agreement/ policy;
- They immediately report any suspected misuse or problem to the Headteacher for investigation/action, in line with the school safeguarding procedures;
- All digital communications with learners and parents/carers are on a professional level and only carried out using official school systems;
- Online safety issues are embedded in all aspects of the curriculum and other activities;
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices;
- In lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc/
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

2f. IT Provider

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that they adhere to and action the following:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy.
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body.
- There is clear, safe, and managed control of user access to networks and devices.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the headteacher for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring systems are implemented and regularly updated as agreed in school policies.

2g. Learners

Learners are responsible for ensuring that they adhere to and action the following:

- Using the school digital technology systems in accordance with the home school agreement and Online Safety Policy.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Knowing what to do if they or someone they know feels vulnerable when using online technology.
- Understanding the importance of adopting good online safety practice when using digital technologies out of school and realising that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

2h. Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website.
- Providing them with a copy of the internet safety information in the home school agreement.
- Publish information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images, cloud services etc.
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in reinforcing the online safety messages provided to learners in school.

2i. Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

3. Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. See Appendix 1 for Reporting and Responding flow chart. The school will ensure the following:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ Abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child Sexual Abuse Material (CSAM)
 - Child Sexual Exploitation Grooming
 - Extreme Pornography
 - Sale of illegal materials/substances
 - Cyber or hacking (offences under the Computer Misuse Act)
 - Copyright theft or piracy
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the MAT.

Where there is no suspected illegal activity, devices may be checked using the following procedures:

- One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- Internal response or discipline procedures;
- Involvement by local authority / MAT (as relevant);
- Police involvement and/or action;
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively;
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident;
- Incidents logged on CPOMs
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.

4. Technology and Security

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements. The responsibility for technical security resides with SLT who may delegate activities to identified roles.

- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT.
- The security of their username and password must not allow other users to access the systems using their log on details.

- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- All school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- The administrator passwords for school systems are kept in a secure place, e.g. school safe.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- The IT service provider is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provide.
- Removable media is not permitted unless approved by the SLT/IT service provider.
- Guest users are provided with appropriate access to school systems based on an identified risk profile.

4a. Mobile Technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

- The school allows the following:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes

¹

Full network access	Yes	Yes	Yes			No
Internet only	No					Yes
No network access	No					Yes

School owned/provided devices:

- All school devices are managed through a central management software.
- There is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed.
- Personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- The use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- Liability for damage aligns with current school policy for the replacement of equipment.
- Education is in place to support responsible use.

4b. Personal Devices

There is a clear policy covering the use of personal mobile devices on school premises for all users - see DEMAT IT Acceptable Use Policy.

4c. Social Media

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff;
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school;

- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information;
- they act as positive role models in their use of social media.

When official school social media accounts are established, there should be:

- a process for approval by senior leaders;
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff;
- a code of behaviour for users of the accounts;
- systems for reporting and dealing with abuse and misuse;
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy. Personal communications which do not refer to or impact upon the school are outside the scope of this policy. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

4d. Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are allowed to take videos and digital images of their own children at school events for their own personal use (as such use is not covered by the Data Protection Act) and only when directed by a member of staff. To mitigate the risk of other children being captured, the school will discourage recording devices during the event and try to allow time and space for individual recordings to be captured of their own children. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- Care should be taken when sharing digital/video images that learners are appropriately dressed.
- Learners must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
- Images will be securely stored in line with the school retention policy.
- Learners' work can only be published with the permission of the learner and parents/carers.

5. Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced.

5a. Filtering

The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.

There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. There is a clear process in place to deal with, and log, requests/approvals for filtering changes. Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon. The school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)

The school has a IT Acceptable Use policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.

Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

5b. Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.

- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:
 - Physical monitoring (adult supervision in the classroom)
 - Internet use is logged, regularly monitored and reviewed
 - Filtering logs are regularly analysed and breaches are reported to senior leaders pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
 - Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
 - Use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

6. Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school via the Multi Academy Trust:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so.
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for.
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- has procedures in place to deal with the individual rights of the data subject.
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier.
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals

affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents

- has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school;
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school;
- only use encrypted data storage for personal data;
- will not transfer any school personal data to personal devices;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

7. Links with other policies

This policy is linked to the:

- Health and safety Policy
- Safeguarding policy
- IT Acceptable Use Policy
- Code of Conduct Policy

8. Appendix 1: Reporting and Responding Flow Chart

