INSPIRE - ENABLE - ACHIEVE

The Vale Federation
E-Safety Policy

This policy was reviewed in December 2023

The policy is to be reviewed by December 2024

Signed:

______________________________ Principal

Date 11th December 2023

1.1 Rationale

The Purpose of this policy is to:

- Set out the key principles expected of all members of the school community at The Vale Federation with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of The Vale Federation.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal, or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary, or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.
- Respect parental consent
- Protect children at risk, without being disadvantaged or excluded
- Prevent significant harm arising to children and young people or serious harm to adults, including the prevention, detection, and prosecution of serious crime.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

1.2 Scope of the Policy

This policy applies to all members of The Vale Federation community (including staff, governors, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of The Vale Federation’s ICT systems, both in and out of The Vale Federation schools.

The Education and Inspections Act 2006 empowers Head of Schools 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 e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The Vale Federation 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 e-safety behaviour that take place out of school.

1.3 Roles and Responsibilities

Role	Key Responsibilities
Principal/Business Director	• To take overall responsibility for e-safety provision. • To take overall responsibility for data and data security (SIRO). • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious esafety incident. • To receive regular monitoring reports/feedback from the IT Department. • To ensure that there is a system in place to monitor and support staff that carry out internal e-safety procedures. • To communicate regularly with SLT and the Designated Safeguarding Lead Governor/Resources Committee to discuss current issues, review incident logs and filtering / change control logs. • Systematically review and develop e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.
Head of School – Designated Safeguarding Lead	• To give permission for photography at school events. • Ensures that e-safety education is embedded across the curriculum. • To communicate regularly with SLT to discuss current issues, review incident logs and filtering / change control logs. • Provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies. • Manage the transition from locked down systems to more managed systems to help pupils/students understand how to manage risk; to provide richer learning experiences; and to bridge the gap between systems at school and the more open systems outside of school (particularly 6th form). • Seek families and pupils' views to develop e-safety strategies.
Safeguarding Officer	• Promotes an awareness and commitment to e-safeguarding throughout the school community.

	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. • To ensure that an e-safety incident log is kept up to date (CPOMS). • Facilitates training and advice for all staff. • Liaises with the Local Authority and relevant agencies. • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Governors	• To ensure that the school follows all current e-safety advice to keep the children and staff safe. • To review the effectiveness of the policy. This will be carried out by the Safeguarding Governor and Resources Committee who will receive regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the Safeguarding Governor will include regular reviews with the Safeguarding Officer/DSL and Business Director (to include e-safety incident logs, actions, and policy enhancements etc.)
Finance & ICT Manager	• To report any e-safety related issues that arises, to the Designated Safeguarding Lead/Business Director. • To ensure regular monitoring reports are compiled and reviewed with the Business Director. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack e.g., keeping virus protection up to date). • To ensure only school devices, with the appropriate security protections can access school servers and protected data areas. • To ensure the security of the school ICT system. • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • The school's policy on web filtering is applied and updated on a regular • That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of school for investigation. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To ensure the hardware and software inventory are kept up to date and any equipment is disposed of appropriately.

	• To complete and assess regular cyber security assessments to measure and review all security protection. • To ensure all devices allocated to specific staff members are signed for using the Device Agreement, detailing the staff members responsibilities and requirements for the devices(s) allocated to them.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. • To ensure any devices allocated to them are kept secure at all times.
All Staff	• To read, understand and help promote the school's e-safety policies and guidance. • To read, understand and adhere to the school staff Acceptable Use / Policy. • To be aware of e-safety issues related to the use of mobile phones, cameras, and handheld devices and that they monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the IT Department. • To maintain an awareness of current e-safety issues and guidance e.g., through CPD. • To model safe, responsible, and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g., email, text, mobile phones etc. • Attend and participate in training provided by the school. • To adhere to all requirements and guidelines stated within the Device Agreement for any IT device allocated to a staff member at all times.
Parents and Pupils where appropriate	• Read, understand, sign, and adhere to the Student / Pupil Acceptable Use Policy (and any other pupils where appropriate). It would be expected that parents / carers would sign on behalf of the pupils) • To understand the importance of reporting abuse, misuse, or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • To help the school in the creation/ review of e-safety policies.
Parents/Carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use which includes the pupils' use of the Internet and the school's use of photographic and video images. • To read, understand and promote the school Pupil Acceptable Use with their children.

	• To access the school website in accordance with the relevant school Acceptable Use. • To consult with the school if they have any concerns about their children's use of technology.
External Groups/Contractors	• Any external individual / organisation will sign a Data Use and Acceptable Use Policy prior to using any equipment or accessing the Internet within school.

1.4 Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Using the schools ICT facilities or equipment for personal use
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic, or discriminatory in any other way.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Senior Leadership team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

1.5 Monitoring Communication

This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

- To establish the existence of facts;
- To ascertain compliance with applicable regulatory or self-regulatory practices or procedures;
- To ascertain or demonstrate effective system operation technically and by users;
- For national security/crime prevention or detection.
- For confidential counselling/support services.
- For Investigating or detecting unauthorized use of the system
- For monitoring communications for the purpose of determining whether they are communications relevant to the business.

- The Vale Federation has an obligation to monitor the use of the internet and e-mail services provided as part of the Broadband service in the schools, in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. The Federation reserves the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process, or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to send and receive electronic communications
- If the email is personal, but related to work, it is good practice to use the word `personal' in the subject header and the footer text should indicate if it is a personal email. The school email should NOT be used for personal emails, unless they are related to the user’s employment.
- Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:
  - ➢ Providing evidence of business transactions;
  - ➢ Making sure the School's business procedures are adhered to;
  - ➢ Training and monitoring standards of service;
  - ➢ Preventing or detecting unauthorised use of the communications systems or criminal activities.
  - ➢ Maintaining the effective operation of communication systems.

1.6 Handling Complaints

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview/counselling by teacher / Head of Department / IT Manager / SLT / Head of school, Principal or Business Director
  - Informing parents or carers;
  - Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system.
  - Referral to Police.
- Our IT Manager acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head of School and/or the Business Director.

• Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection policy and procedures.

1.7 Review and Monitoring

The e-safety policy is referenced from within other school policies: Child Protection policy, AntiBullying policy, Remote Learning policy and Behaviour policy.

• The school has an IT Manager who will be responsible for document ownership, review, and updates.
• The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
• The e-safety policy has been co-written by the IT Manager, Business Director, Principal and Data Protection Officer is current and appropriate for its intended audience and purpose.
• There is widespread ownership of the policy, and it has been agreed by the SLT. All amendments to the school e-safety policy will be discussed in detail with all members of teaching staff.

1.8 Education and Curriculum

Student e-safety curriculum

The Vale Federation:
• Has a clear, progressive e-safety education programme as part of the curriculum. It is built on LA e-safeguarding and national guidance. This covers a range of skills and behaviours appropriate to their age, experience, and abilities, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To know how to narrow down or refine a search;
- For older pupils to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- To understand acceptable behaviour when using an online environment / email, i.e., be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs, and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will ‘groom’ young people for sexual reasons;

- To understand the impact of cyber bullying, sexting, and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyber bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e., parent or carer, teacher or trusted staff member, or an organisation such as Child Line or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network. Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and Governor training

The Vale Federation:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program;
- Provides, as part of the induction process, all new staff, including those on university/college placement and work experience, with information and guidance on the e-safety policy and the school's Acceptable Use Policies.

Parent awareness and training

The Vale Federation:

- Runs a rolling programme of advice, guidance, and training for parents, including:
  - Introduction of the Acceptable Use to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school web site;
  - Suggestions for safe Internet use at home;
  - Provision of information about national support sites for parents.

1.9 Expected Conduct and Incident Management

Expected conduct

At The Vale Federation, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy;
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school;
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras, and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

- Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and handheld devices.

Students/Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use information at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

At the Vale Federation:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g., the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's SLT and Governors.
- Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

1.10 Managing the ICT Infrastructure

Information system security:

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The Vale Federation uses Broadband with its firewall and filters.
- Portable media may not be used at any time
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The IT Manager will review system capacity regularly.

E-mail:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- The forwarding of chain letters is not permitted.
- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is `Confidential' in the subject line Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.

Published content and the school web site:

- The contact details on the Web site should be the school address, e-mail, and telephone number.
- Staff or pupils' personal information will not be published.
- The Principal and Business Director will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Photographs published on the website do not have full names attached.
- The school website complies with the statutory DfE guidelines for publications

Publishing pupil's images and work:

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by full name.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission/consent from parents or carers will be obtained before photographs/videos of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.
- Images of staff should not be published without annual consent
- Acceptable Use Policy

Password policy:

- All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.
- Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
- **Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.**
- All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

• All staff passwords will be required to be changed every 90 days to improve security. This is automated.

Staff:

• Staff can only use the Federations email system via the school system
• Staff only use Federations email system for professional purposes
• Access in school to external personal email accounts may be blocked
• Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

> • The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
> • The sending of chain letters is not permitted;
> • Embedding adverts is not allowed;

• All staff sign our 'Acceptable Use' Policy to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Social networking and personal publishing – also see Section 2 of the IT Acceptable Use Policy for the Social Networking Policy:

• Social networking sites and newsgroups will be blocked unless a specific use is approved by the Business Director and the Data Protection Officer.
• Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests, and clubs etc.
• Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g., house number, street name, school, or shopping centre.
• Teachers are advised not to run social network spaces for students on a personal basis.
• Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals, and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
• Students should be advised not to publish specific and detailed private thoughts.
• The Vale Federation staffs are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Managing filtering

• The Vale Federation will work in partnership with JSL to ensure filtering systems are as effective as possible.
• If staff or pupils discover unsuitable sites, the URL, time, and date must be reported to the IT Manager, IT Department, or a member of SLT.
• The IT Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.
• Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (addresses later).

Managing emerging technologies

• Emerging technologies will be examined for educational benefit and a risk assessment (DPIA) will be carried out before use in school is allowed.

- Staff will be issued with a school phone where contact with pupils is required during school activities. All SLT, Safeguarding Officer and the Site Manager have school mobile phones.
- Staff who work with pupils out of school hours and use their personal phones to contact parents should inform the Head of school or Principal for authorisation.

Protecting personal data

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998.

Authorising Internet access

- The Vale Federation will maintain a current record of all staffs that are granted Internet access.
- All users must read and sign the school policy on Acceptable Use.
- In all Key Stages, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Pupils will use age - appropriate search engines and online tools and online activities will be teacher directed.
- Parents will be informed that pupils will be provided with supervised Internet access.

1.11 Data Security

Strategic and operational practices

At the Federation we ensure:

- Staff know who to report any incidents where data protection may have been compromised
- All staff are DBS checked and records are held in one central record

This makes clear staffs' responsibilities with regard to data security, passwords, and access.

We follow guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services, Health, Welfare and Social Services.

We ask staff to undertaken at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files, and devices.

These access rights are managed by the IT Department. All requests for changes to access must be authorised by the Business Director, in collaboration with the Data Protection Officer.

Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT technician immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Business Director.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT service provider/etc.

Technical Solutions

Staff have secure area(s) on the network to store sensitive documents or photographs.

We require staff to log-out of systems when leaving their computer, but also enforce lock-out after a short period of idle time.

We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.

All servers are in lockable locations and managed by DBS-checked staff.

1.12 Asset Disposal

Details of all school-owned hardware will be recorded in a hardware inventory. Details of all school-owned software will be recorded in a software inventory. All redundant equipment will be 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.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen. Disposal of any 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.