SCHEDULE 12: SECURITY POLICY

The HMG Policy Framework April 2014 as at the Effective Date forms the content of this Schedule 12. This and any updates to it following the Effective Date can be found at the following web link. Where the Supplier is unable to access the links, it shall request the HMG Policy Framework April 2014 from STA and STA shall make the same available to the Supplier upon such request :

https://www.gov.uk/government/publications/security-policy-framework

Version 1.1 – May 2018

Cabinet Office

HMG Security Policy Framework

Version 1.1 - May 2018

Version History

Document Version	Date Published	Summary Of Changes
1.0	April 2014	N/A
1.1	May 2018	Minor amends – Changes in Data Protection legislation (GDPR).

Foreword

Sir Jeremy Heywood – Cabinet Secretary
Chair of the Official Committee on Security (SO)

As Cabinet Secretary, I have a good overview of the many excellent services the Civil Service is responsible for, and of course the wide range of challenges that we need to manage to deliver them.

The right security, appropriately tailored to take proper account of the very wide range of different jobs we do, assets we handle and environments we work, is a critical pre-requisite for meeting many of these challenges. It ensures we can keep and develop the public's trust that we will handle their information properly, advise Ministers in confidence, and protect the many commercial and financial interests we are responsible for. And of course, it helps maintain national security.

Getting security right has never been more important as the Civil Service continues to modernise and improve our ways of working, and deliver more and more services online. There are longstanding threats and risks to bear in mind; but we must also continue to develop our growing appreciation of global and cyber challenges, critical infrastructure dependencies, together with wider resilience and sustainability issues.

Responsibility for the security of government is delegated down from the Prime Minister and Cabinet to me, as Cabinet Secretary and Chairman of the Official Committee on Security, and then to Heads of Department. It is important therefore to understand our expectations which are set out very clearly in this Security Policy Framework. It should be applied across HMG, but also in respect of assets that are held by third parties in the wider public sector and by our commercial partners.

The Framework incorporates the new Classification Policy launched this month and I am pleased that it makes much throughout of the importance of proper, meaningful engagement of all staff on security matters. No matter how much technology develops people remain our strongest asset. So proper management, good judgment and discretion remain the most effective security protection. The emphasis upon personal responsibility and accountability that underpins the new policy is a key feature of the Framework, and reflects the same obligations that the Civil Service Code places upon us all.

I invite all Boards to act on the introduction of this new Framework and to bring it to the widest attention of colleagues and partners.

SIR JEREMY HEYWOOD

Cabinet Secretary
April 2014

The Security Policy Framework

The Prime Minister is ultimately responsible for the overall security of HMG. They are supported by the Cabinet Secretary, who chairs the Official Committee on Security (SO). Across HMG responsibility for the security of organisations lies with the respective Ministers, Permanent Secretaries and Management Boards.

This Framework describes the Cabinet Secretary and SO's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.

Overarching Principles

There are some principles common to every area of security:

1. Protective security should reflect the UK's widest national security objectives and ensure that HMG's most sensitive assets are robustly protected.

2. Security must enable the business of government and should be framed to support HMG's objectives to work transparently and openly, and to deliver services efficiently and effectively, via digital services wherever appropriate.

3. Risk management is key and should be driven from Board level. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to people, information and infrastructure to an acceptable level. This process will take full account of relevant statutory obligations and protections, including data protection legislation, the Freedom of Information Act, the Official Secrets Act, Equality Act, and the Serious Organised Crime and Police Act.

4. Attitudes and behaviours are fundamental to good security. The right security culture, proper expectations and effective training are essential.

5. Policies and processes will be in place for reporting, managing and resolving any security incidents. Where systems have broken down or individuals have acted improperly, the appropriate action will be taken.

Security Outcomes

The Cabinet Secretary and SO expect all HMG organisations (and partners handling HMG information) to meet a range of mandatory security outcomes described below. These outcomes do not specify particular processes but describe what good security will look like. HMG organisations will consult the full range of policy, advice and guidance provided by the Cabinet Office, Centre for the Protection of National Infrastructure, National Cyber Security Centre, and other sources of good practice to shape their business specific approaches, mindful that:

- Government organisations know their own business best, including how local risks should be managed to support operations and services.
- Permanent Secretaries/Heads of Department are accountable to Parliament for the security of their organisations.
- An annual reporting process (the Security Risk Management Overview) will ensure compliance and an appropriate level of commonality across government.

Good Governance

Effective leadership is a critical component of good security and accountability. The Permanent Secretary (or equivalent) will own the organisation's approach to security and ensure that these issues receive the attention and investment required.

Government organisations will have:

a. An appropriate security governance structure to support the Permanent Secretary, that is properly resourced with individuals who have been appropriately trained. These include:

- A Senior Information Risk Owner (SIRO).
- A Departmental Security Officer (DSO) who can manage day-to-day protective security.
- Information Asset Owners (IAOs) across distinct business units.
- Information risk assessment and risk management specialists.

- Other specialists relevant and specific to the organisation's needs.

b. Board-level oversight of security compliance and auditing processes.

c. Arrangements to determine and satisfy themselves that Delivery Partners, service providers and third party suppliers, apply proper security controls too (including List X accreditation for companies handling SECRET assets).

Culture and Awareness

Everyday actions and the management of people, at all levels in the organisation, contribute to good security. A strong security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation will allow the business to function most effectively.

Government organisations will have:

a. A security culture that supports business and security priorities and is aligned to HMG's overarching priorities and the organisation's own appreciation of risk.

b. Training which encourages personal responsibility and good security behaviours.

c. Processes, systems and incentives to deliver this.

d. Mechanisms to drive continuous improvement, tackle poor and inappropriate behaviour, enforce sanctions and encourage the sharing of best practice.

Risk Management

All HMG activities attract risk. Risks need to be assessed by government organisations so that they can make informed, practical and effective business enabling decisions.

Government organisations will have:

a. A mature understanding of the security risks throughout the organisation,

where appropriate this will be informed by the National Technical Authorities.

b. A clearly-communicated set of security policies and procedures, which reflect business objectives to support good risk management.

c. Mechanisms and trained specialists to analyse threats, vulnerabilities, and potential impacts which are associated with business activities.

d. Arrangements to determine and apply cost-effective security controls to mitigate the identified risks within agreed appetites.

e. Assurance processes to make sure that mitigations are, and remain, effective.

Information

The security of information is essential to good government and public confidence. To operate effectively, HMG must maintain the confidentiality, integrity and availability of its information.

Government organisations will have:

a. Staff who are well trained to exercise good judgement, take responsibility and be accountable for the information they handle, including all partner information.

b. Mechanisms and processes to ensure assets are properly classified and appropriately protected.

c. Confidence that security controls are effective and that systems and services can protect the information they carry. There will be an overarching programme of information assurance driven by the Board.

Technology and Services

The delivery of efficient public services, including the proper protection of citizen data, requires modern and functional technology. Resilience to cyber threats, compliance with data protection laws and management of national security-related information within these systems will require security to be integral to their design and implementation.

Government organisations will have:

a. Identified if technology and services are Critical National Infrastructure, and risk manage accordingly.
b. Risk-informed security controls which:

- Mitigate applicable threats.
- Are kept current and actively managed.
- Protect against, detect and correct malicious behaviour.
- Ensure that critical technology and services are resilient to disruptive challenges such as cyber attacks, and have the means to recover from these.

Personnel Security

People are an organisation's most important asset, so personnel assurance is fundamental to good security. Government organisations will deliver the appropriate combination of recruitment checks, vetting and on-going personnel security management to be assured, and to remain assured, about their people and to mitigate the risks from well-placed insiders.

Government organisations will have:

a. Joined-up HR and personnel security policies and processes, including recruitment checks (the Baseline Personnel Security Standard (BPSS)) for those with access to HMG assets.

b. Processes to evaluate areas of particular insider risk which require corresponding and proportionate levels of vetting.

c. Robust arrangements for managing the delivery of vetting services, and mechanisms to handle appeals.

d. Effective aftercare arrangements that include regular security appraisals, promote a security conscious culture, and drive staff and line management engagement.

Physical Security

Appropriate physical security measures will ensure a safe and secure working environment for staff that can protect against a wide range of threats (including theft, terrorism or espionage).

Government organisations will have:

a. Processes and plans in place, including those developed from the early stages of building design, to determine the appropriate physical security requirements through planning and risk assessment.

b. Mechanisms to implement internal and external security controls in a layered fashion that deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack.

c. Substantial controls for controlling access and proximity to the most high risk sites and Critical National Infrastructure assets.

Preparing for and Responding to Security Incidents

Well-tested plans, policies and procedures will reduce organisations' vulnerability to security incidents (especially from the most serious threats of terrorism or cyber attack), but also leaks and other disruptive challenges.

Government organisations will have:

a. Business continuity arrangements aligned to industry standards, to maintain key business services, building resilience and security to facilitate a rapid and effective response to recover from incidents.

b. Processes in place to regularly conduct risk and vulnerability assessments and review resilience planning for critical assets, particularly those identified as Critical National Infrastructure.

c. Counter-terrorism contingency plans in place setting out procedures to be followed in the event of a terrorist threat, including procedures to immediately adjust security requirements around the Government Response Level system.

d. Effective management structures that ensure shared communications between HR and security teams and provide policies and procedures for

detecting, reporting, responding to and handling incidents, including disciplinary measures that are well communicated and understood by staff.

e. Reporting mechanisms to the Cabinet Office Government Security Group, regarding incidents of unauthorised disclosure and breaches of official information, including incidents concerning classified information from foreign governments, agencies or organisations. In addition, such mechanisms should also exist to the Information Commissioner's Office for if and when a serious loss or breach of personal data occurs, in line with data protection legislation.

Policy Priorities

Protective security should always be approached in the round (holistically), but it is helpful to bear in mind specific areas of information, physical and people security. HMG policy across these three areas is set out below:

Information Security

All information that HMG deals with has value. HMG handles the wide variety of information that it generates, collects, processes, stores and exchanges appropriately to ensure: the confidentiality of citizen data and commercial information; good government and the effective and efficient delivery of public services; the proper protection of national security-related information; and that obligations to international partners are met. HMG expects its' partners in the wider public sector, suppliers and other commercial partners who handle information on HMG's behalf to do the same.

HMG operates a Classification Policy to identify and value information according to its sensitivity and to drive the right protections. This comprises three levels: OFFICIAL, SECRET and TOP SECRET for which there are distinct security arrangements. OFFICIAL covers most of the day-to-day business of government, service delivery, commercial activity and policy development.

SECRET and TOP SECRET information will typically require bespoke, sovereign protection, but OFFICIAL information can be managed with good commercial solutions that mitigate the risks faced by any large corporate organisation. In this way government can deliver securely and efficiently, and shape its services to meet the user needs.

The effective management of information is critical to safeguarding it. Government organisations will consider good information management practice as the basis for their information security arrangements.

Technology and Services

HMG will deliver services to the public digitally wherever it can. These services must be designed and delivered securely. A Public Services Network (PSN) offers an infrastructure across the public sector to increase efficiency and reduce overall expenditure. Organisations will utilise appropriate technologies (including mobile

devices) and services (including Cloud) and secure these by default wherever possible. Contracts will specify security requirements clearly.

For new policies or projects that include the use of personal information, an initial assessment on the privacy risks to individuals in the collection, use and disclosure of the information, is made. All ICT systems that manage government information or that are interconnected to them are assessed to identify technical risks. Proportionate assurance processes will provide confidence that these identified risks are being properly managed. This also takes account of risks originating from within the organisations, which could arise from poor behaviours and malicious insiders.

Accountability

HMG organisations are responsible for the information they handle under appropriate governance structures, including at Board level lead. A SIRO is accountable and responsible for information risk across the organisation, supported by IAOs from distinct business units. The SIRO will ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately. HMG continues to remind the public of the importance of protecting their own information online and when accessing government services.

Physical Security

HMG has a wide, diverse estate at home and abroad, including administrative HQs, military bases, Embassies, public offices, and service centres. To ensure: the proper protection of citizen data, commercial confidences, and national security related information; good government and the efficient delivery of public services; and a safe working environment for staff and visitors, a range of physical security controls are required. HMG assets held or managed by third parties must be similarly protected.

The range of physical controls will vary depending upon circumstances and business requirements, and the type of threats (including natural hazards, other disruptive challenges, crime, terrorism, and espionage). Organisations will layer their security, including: perimeter controls and guarding; building design features; limiting, screening or otherwise controlling access; appropriate fittings and office furniture; and the use of separate areas in buildings for particularly sensitive work. Controls should not be onerous but proportionate to ensure the safety and security of staff and visitors.

HMG organisations should also have in place arrangements to adapt and enhance security measures if there is an increase in threats, especially from terrorism. In such circumstances, it may be necessary to limit non-essential access; to increase the frequency of staff and visitor checks and bag searches; and to establish additional

perimeter controls and other guarding activities. Response mechanisms and contingency plans are in place to respond to possible critical security incidents and to enable the continuity of services.

Personnel Security and National Security Vetting

Personnel security controls confirm the identity of individuals (employees and contractors) and provide a level of assurance as to their trustworthiness, integrity and reliability. Whilst HMG personnel security controls cannot provide guarantees, they are sensible and important precautions.

It is HMG's policy that all areas of government and the national infrastructure should include in their recruitment processes certain basic checks. These checks include verification of the applicant's identity, employment history, their right to work in the UK and, if appropriate, checks of any unspent criminal records. Within government these controls are described in the Baseline Personnel Security Standard.

National Security Vetting

National security vetting comprises a range of additional checks and may be applied where policy or a bespoke risk assessment indicates it is proportionate to do so. The risk assessment process takes account of the access an individual may have to sensitive assets (physical, personnel or information) at risk from a wide range of threats. These threats will include: terrorism, espionage, or other actions that could threaten the UK.

There are three different types of national security vetting clearance: Counter-Terrorist Check (CTC), Security Check (SC), and Developed Vetting (DV). Before any such clearance is undertaken the requirements of the Baseline Personnel Security Standard must be met. Whilst the information required and the range and depth of checks undertaken at each level may vary, they are all intended to allow Government departments and agencies, the Armed Forces and police forces to assess whether individuals who are to be employed in sensitive posts or critical functions might represent a security risk either directly or indirectly.

Ongoing Personnel Security Management

The national security vetting process provides an assessment of the vetting subject at the time the process is carried out, but active, ongoing personnel security management is required to ensure that a security clearance maintains its currency. As a minimum, this will involve active consideration of the vetting subject's continuing conduct in respect of security matters; it will also require checks to be repeated at regular intervals.

AJT

Any enquiries regarding this publication should be sent to us at GSSmailbox@cabinet-office.x.gsi.gov.uk

You can download this publication from www.gov.uk.

Standards
& Testing
Agency

TEST OPERATIONS SERVICES

Services Agreement for the Delivery of Test Operations Services

---

Volume 3

Schedules 13 to 21

1 Introduction

We understand that unfortunately things can occasionally go wrong or that expectations are not always met. When this happens we need to understand the difficulties faced so that we can investigate the circumstances leading to the complaint and as appropriate:

- Improve the standard of services we deliver
- Put things right when they have gone wrong
- Learn from our mistakes
- Where things are beyond our control – explain our remit, limitations and seek to improve our communication to set expectations appropriately.

The aim of this policy is to provide a fair, consistent and structured process for our customers if they are dissatisfied with the service they have received. Emphasis will be placed on resolving complaints as quickly as possible. This policy is compliant with the Department for Education's complaints policy: more information can be found at https://www.gov.uk/government/organisations/department-for-education/about/complaints-procedure.

We equip our staff to deal with complaints efficiently and effectively, and where applicable, lessons learnt from complaint investigations will be used to directly inform service improvements.

2 What is a complaint?

A complaint is any expression of dissatisfaction about a service provided pursuant to, or a member of staff acting on behalf of Capita Business Services Ltd in respect of, the delivery of the Services. This could be a failure to do what we said we would do, or perhaps you are unhappy with the way you were treated. Examples of a complaint include:

- A failure to provide an offered service
- Giving incorrect or misleading information
- Rude, unhelpful or inappropriate behaviour by staff
- Poor communication.

Unfortunately, we cannot handle complaints that fall in to the following categories:

- Relating to a specific policy (these must be directed to a Minister or your MP or the STA)
- Queries associated with a specific Key Stage 1, Key Stage 2 or Phonics test paper
- Complainants who use obscenities, racist or homophobic language or who are personally abusive about members of staff.

3 Our commitment

We are committed to learning from our mistakes as part of our drive for continuous improvement. We will:

- Take all complaints seriously
- Follow an open and transparent process
- Provide a timely and meaningful response
- Audit our complaints policy and procedures on a regular basis
- Analyse the types of complaints we receive to look for trends, areas of high risk and for opportunities to improve our services.

4 How will my complaint be handled?

In many cases, misunderstandings can be resolved quickly by speaking with a manager. Where you feel that this is inappropriate and that your problem needs to be looked at in a more formal capacity you can make a formal complaint.

When dealing with complaints we will:

- Log your complaint and assign a reference number
- Send an acknowledgement by email within one Business Day of receipt
- Respond to your concerns within 10 Business Days
- Complaints will be investigated by the relevant department
- Should we consider that a conflict of interest exists, another department manager will be allocated the complaint to investigate

In all cases, the outcome of your complaint will be communicated to you in writing.

We will record complaints (and compliments) in a feedback database which we will review at our Continuous Improvement Forum.

5 What if I am still dissatisfied?

If you are unhappy with the way your complaint has been handled you:

- May request a review of the complaint by writing to the Managing Director, Test Operations Service, providing your complaint reference number
- You must state why you are unhappy and what your expected outcome of the complaint would be
- A Complaint Review will take place within 10 Business Days of receiving a valid request
- The Complaint Review will be conducted by a Complaint Review Team consisting of Senior Managers
- The Complaint Review outcome will be communicated to you in writing within two business days of the review.

6 Publication of complaints digest

As part of our commitment to continuous improvement, we will publish an annual digest of complaints received in respect of the Test Operations Services. The digest will include as a minimum the following information:

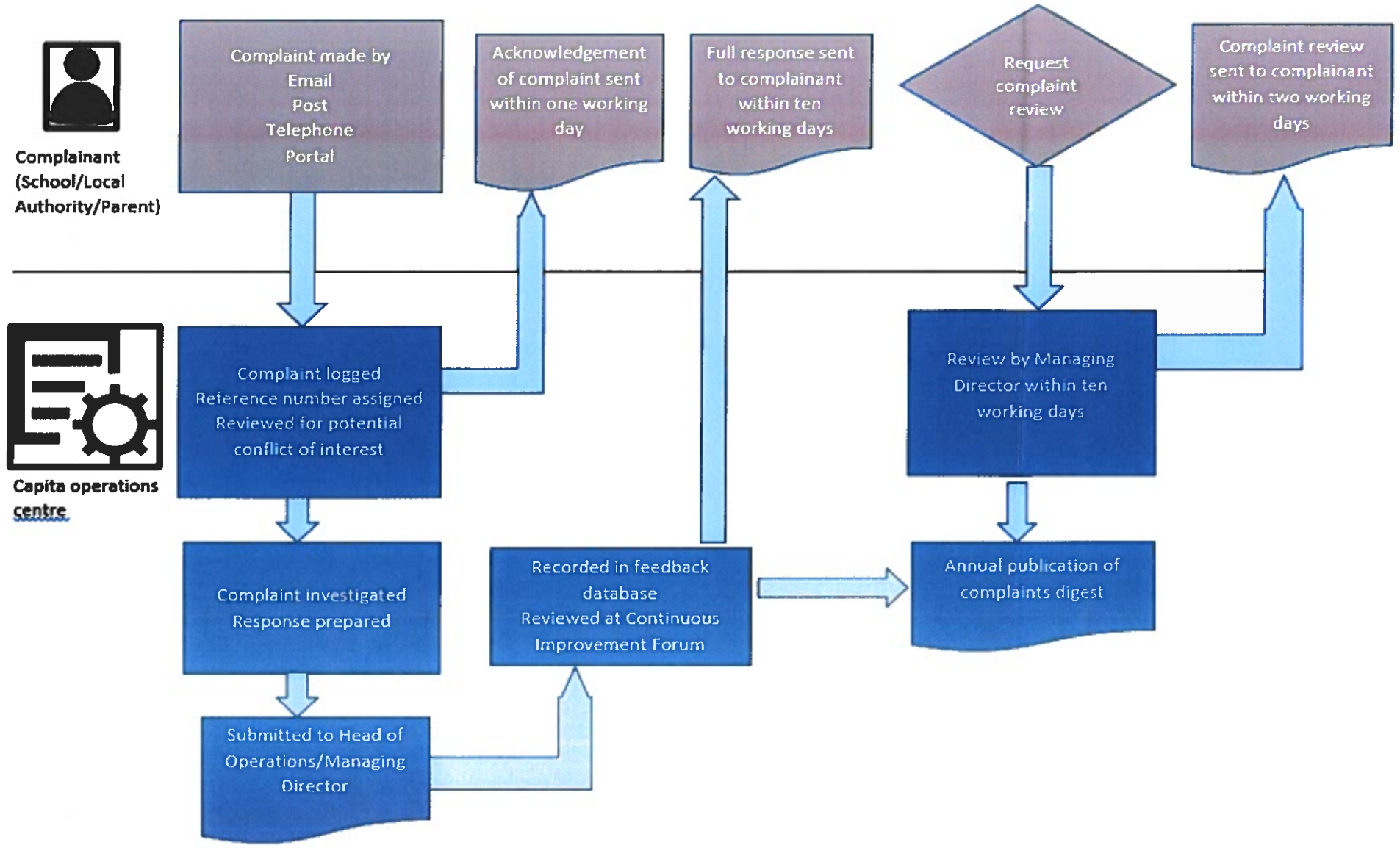
- Number of complaints received by category (for example late response/staff/technical problem)
- Remedial actions taken to rectify the complaint
- Average time taken from receipt of complaint to closure
- Recommended steps to prevent recurrence.

7 Vexatious complaints

If we believe an individual or organisation is pursuing a complaint that is hindering our ability to deal with other complaints, is unreasonably persistent and refuses to co-operate with our process, we may invoke our vexatious complaints procedure. We will refer all complaints that may fall under this category to the Standards & Testing Agency before confirming the status as a vexatious complaint to the complainant.

8 Privacy notice

We will only use the information we collect to deal with a complaint to investigate the root causes of the complaint and to respond to the complainant. We will strive to preserve the anonymity of a complainant but there may be exceptional circumstances in which we will need to identify a complainant by name. We will not share information about you with third parties without your consent unless the law requires us to.


Complainant (School/Local Authority/Parent)
Complaint made by
Email
Post
Telephone
Portal
Acknowledgement of complaint sent within one working day
Full response sent to complainant within ten working days
Request complaint review
Complaint review sent to complainant within two working days
Capita operations centre
Complaint logged
Reference number assigned
Reviewed for potential conflict of interest
Review by Managing Director within ten working days
Complaint investigated
Response prepared
Recorded in feedback database
Reviewed at Continuous Improvement Forum
Annual publication of complaints digest
Submitted to Head of Operations/Managing Director

SCHEDULE 14: BRAND GUIDELINES

As at the date of this Agreement, STA's Brand Guidelines comprise the documents below, namely, **"How to use Branding in the Department and its Executive Agencies"** and **"DfE's writing style guide"**. During the Term, these documents may be updated from time to time by the Department for Education and where they are so updated, STA shall make the same available to the Supplier. Such updated versions of the documents shall replace and supersede in their entirety, the documents that can be found below as at the date of this Agreement:

SCHEDULE 14: BRAND GUIDELINES

As at the date of this Agreement, STA's Brand Guidelines comprise the documents below, namely, **"How to use Branding in the Department and its Executive Agencies"** and **"DfE's writing style guide"**. During the Term, these documents may be updated from time to time by the Department for Education and where they are so updated, STA shall make the same available to the Supplier. Such updated versions of the documents shall replace and supersede in their entirety, the documents that can be found below as at the date of this Agreement:

Department
for Education

How to use branding in the Department and its executive agencies

A guide for staff – April 2013

Contents

Introduction

The Department's brand identity is like our official signature, so it's important to use this in the correct way on all communications – whether for our own staff or people outside the organisation. This guide sets out some of the basic rules to make sure that our communications are clear and consistent every time. This is so people can quickly see that a document or other communication comes from the Department and that it's official.
The Department and our three executive agencies all use the same style of branding. This features the Royal Coat of Arms to indicate our status as part of Government. There are specific versions of this logo for the Department for Education, Education Funding Agency, Standards and Testing Agency, and the National College for Teaching and Leadership. You can see the different versions at a glance below.

You may be glad to know that we've produced some simple templates for the most common uses of our brand. You can download a Word document, Powerpoint slide presentation and letterhead templates from the intranet.

Where to get help or advice
Hopefully you will find everything you need in this guide. But if you have any questions or need a copy of these logos for any other use, please email Publishing Team at: Publishing.TEAM@education.gsi.gov.uk

Some basic brand principles

The style and design elements shown in this guide are the only ones that should be used for Department for Education and executive agency corporate communications. There are two important principles behind the Department's approach to branding:

- We should always aim to make things clear and consistent for our audience
- We should minimise costs and reduce bureaucracy wherever possible **Which logo should I use?**
- We always use the Department's brand to communicate with people about policy issues
- We can use the relevant executive agency's logo for communications relating directly to their business – but where more than one agency is featured it's usually better to use the Department's logo rather than having multiple logos for each agency We never create or use separate logos or sub-brands for individual directorates, teams or units.

Branding for campaigns or services
Very occasionally we may need to use a different brand to communicate directly with members of the public – for example a sustained campaign to change people's behaviour or introduce a new product or service. You must always get specific approval from Communications Group for this.

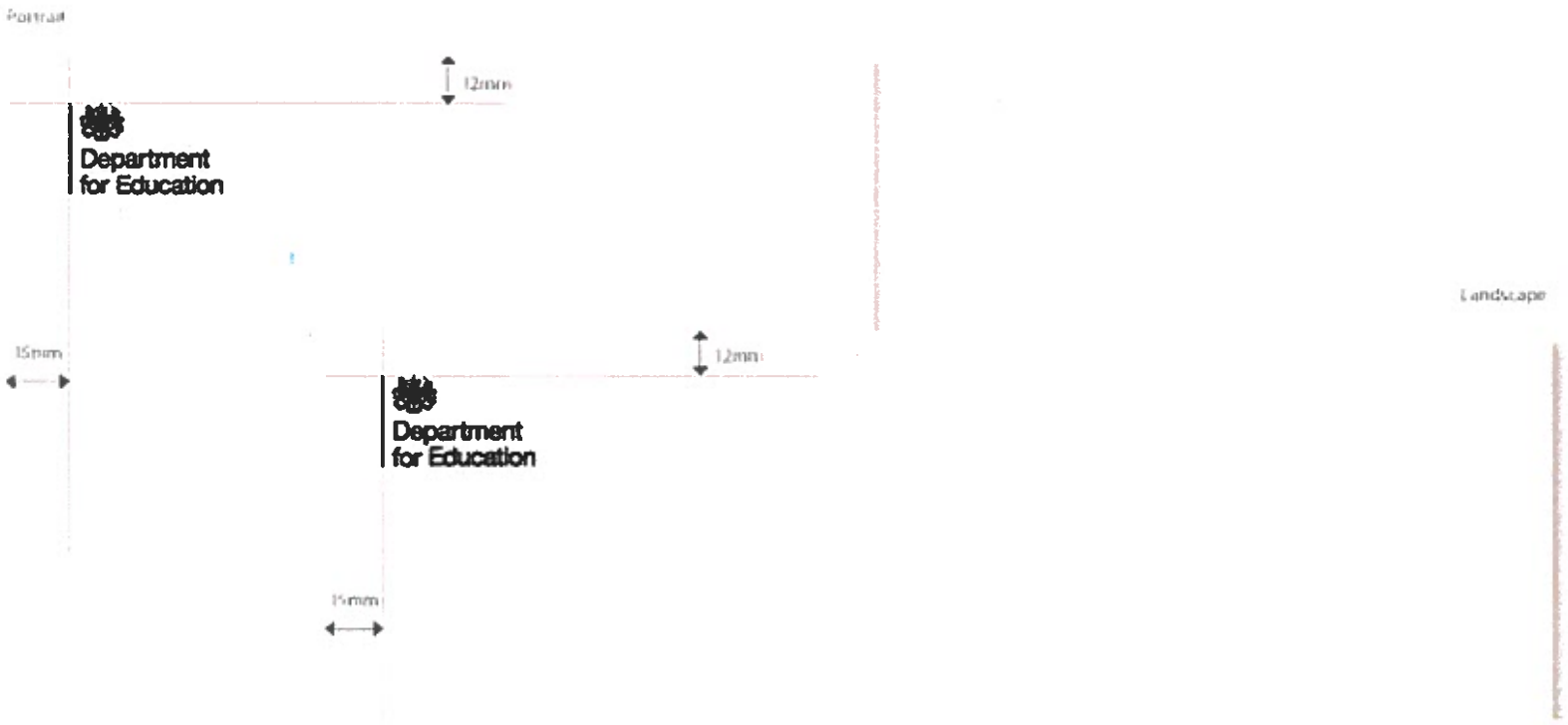
Endorsements

The Department's logo should never be used as a general endorsement for third-party organisations, services or programmes. Where appropriate, though, it can be used by our partners to indicate a funding or contractual arrangement, or some other occasion when we are directly involved or share responsibility for delivery. The extent of the endorsement should be accurately reflected in how the logo is used – for example alongside text to make clear that a particular initiative is 'supported by', 'funded by', and so on. You should always seek approval from Communications Group before allowing others to use the DfE or executive agency logos.

Logos – positioning

The Department's (and agencies') brand identities are made up of a number of important parts. It's the main way we identify ourselves, so it's important that it always appears in the same way. Only the original artwork should be used. You must never redraw or alter this in any way.

Positioning
Because our logo features the Royal Crest, there are some important rules on how this should be used. Our Word templates already have the logo in place.
If you are commissioning new design work, the logo should normally appear at the top left of our communication, so that it has supremacy over all other content. There should be a reasonable margin (see below):



If for any reason this isn't possible you should contact the branding team for guidance.

Logos – exclusion zone and size

Exclusion zone

The exclusion zone is a distance equivalent to the width of the Royal Coat of Arms around the identity (x in the figure below). This is the minimum clearance; whenever possible, leave more space around the identity than the exclusion zone.

Size
If you need to use a logo somewhere not covered by the templates, please ensure that the minimum size is 30mm tall (for DfE and NCTL) or 35mm tall (for EFA and STA).
Minimum sizes for online use are 125 pixels high (for DfE and NCTL) or 150 pixels high (for EFA and STA).

Colours

Colour can play an important role in bringing communications to life, but only certain colours can be used on DfE and executive agency material. Using these correctly helps people to become familiar with our communications as well as making them easier to read.
You will need to use the specific colour references shown when producing something in our style.
Our main colour is the blue shown below. This is the same colour which features in our logo.

Blue

RGB R16 G79 B117 **CMYK** 96c 69m 32y 15k **Pantone** 2955

We have five supporting colours which can also be introduced to add variety. Aim to use just one of these in each communication plus black for the main text.

Red	Orange	Yellow	Green	Purple
RGB R138 G37 B41 **CMYK** 45c 100m 100y 15k **Pantone** 484	**RGB** R232 G125 B30 **CMYK** 0c 59m 100y 5k **Pantone** 1595	**RGB** R194 G162 B4 **CMYK** 0c 15m 100y 28k **Pantone** 457	**RGB** R0 G71 B18 **CMYK** 79c 0m 100y 75k **Pantone** 350	**RGB** R38 G8 B89 **CMYK** 91c 100m 0y 49k **Pantone** 2695

Colours – tints and shades

On the inside of documents, the colours can also be used as tints – ie different strengths of the same colour. You can use our colours at 20 per cent variations of their original strength – ie at 100, 80, 60, 40 or 20 per cent.

	Blue	Red	Orange	Yellow	Green	Purple
100%						

	RGB R16 G79 B117	**RGB** R138 G37 B41	**RGB** R232 G125 B30	**RGB** R194 G162 B4	**RGB** R0 G71 B18	**RGB** R38 G8 B89
80%	**RGB** R64 G114 B145	**RGB** R161 G81 B84	**RGB** R237 G151 B75	**RGB** R206 G181 B54	**RGB** R51 G108 B65	**RGB** R81 G57 B122
60%	**RGB** R112 G149 B172	**RGB** R185 G124 B127	**RGB** R241 G177 B120	**RGB** R218 G199 B104	**RGB** R102 G145 B113	**RGB** R125 G107 B155
40%	**RGB** R159 G185 B200	**RGB** R208 G168 B169	**RGB** R246 G203 B165	**RGB** R231 G218 B135	**RGB** R153 G181 B160	**RGB** R168 G156 B189
20%	**RGB** R207 G220 B227	**RGB** R232 G211 B212	**RGB** R250 G229 B210	**RGB** R243 G236 B205	**RGB** R207 G218 B189	**RGB** R212 G206 B222

If you are using a tint on a page, you should always use the solid colour as well.
You may use black or solid colour for text in headings and sub-headings – never use a tint as this can make the text harder to read.
Only use black text for main body copy.
If you need to use white text for some reason (for example, in a coloured box for a quote or case study), make sure the background colour is dark enough to provide sufficient contrast.

Typefaces

We use three different typefaces on DfE and executive agency communications:

Helvetica Neue **Myriad**

ABCDEFGHIJKLM
NOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890
?!@&#$%

ABCDEFGHIJKLM
NOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890
?!@&#$%

Arial

ABCDEFGHIJKLM
NOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890
?!@&#$%

Professionally produced material should use Helvetica Neue for headings and Myriad for other text.

If you're creating something yourself, for example an email or Word document, and cannot use either of these typefaces, then you should use Arial throughout.
NOTE: It's also fine to use Calibri or Tahoma in emails – as long as it is a black, regular sans serif typeface in keeping with our normal look and feel.

Making sure people can read the type

We must always make sure that text is legible in our communications. To help with this, keep in mind the following guidance.

Type size and weight
The size of type is fundamental to whether people can or will read our communications. We recommend a type size between 12 and 14 point. The larger the type size, the more people will be able to read this. Avoid light type weights.

Type styles
Where you need to emphasise key words, use bold. Blocks of capital letters, underlined or italicised text are all harder to read. Minimal use of capital letters is fine - but avoid using them for continuous text. Never underline text.

Word spacing and alignment
Keep to the same amount of space between each word. Do not condense or stretch lines of type. Set text ranged left and avoid fully justified text as this can be harder to read.

Setting text
Vertical text can be extremely difficult to follow, so always set text horizontally. For the same reason avoid fitting text around images if this means that lines of text start in a different place and are therefore difficult to find. Avoid setting text over images as this will affect the contrast.
Columns can sometimes be easier to read because they make each line shorter. Bear in mind that most of our communication is now in the format of online PDFs, where two columns (or more) may force the reader to keep scrolling up and down to read a page.

Navigational aids
Consider using plenty of white space to make each page easier to read, especially between paragraphs and sections. It is usually helpful for readers if recurring features such as headings and page numbers are always in the same place.

Language

Using a consistent language and tone helps people form a consistent view of who we are, what we do and how we want to engage with people.
This is every bit as important as following a consistent design style. We must use plain English and write as clearly and concisely as possible. Avoid using acronyms and abbreviations unless they are already familiar to your reader.

When using the Department's or executive agencies' names, always use capital initials and always spell these out in full the first time. You can abbreviate these to 'the Department' or 'the Agency' as appropriate afterwards.
You can get further guidance on our writing style from the intranet.

Photography

People are at the heart of our organisation and many of our policies and activities are highly visual. We don't normally use photography on documents which are designed for printing as this pushes up cost. However, it's fine to use photography on other material such as online communications. Photographs can also be used sparingly on internal spreads. They can illustrate a key point or show a case study in action. Don't try to do too much. Simplicity is key and an image should always be relevant and add something to your message. Whatever you're producing, try to choose an image that captures a real moment in time – something which is natural, authentic and relaxed.

When choosing photography ask yourself:

- Does it reflect your audience or subject?
- Does it support the key message?
- Does it convey empathy?
- Does it feel real?

Do not use:

- black and white or duotone images
- montages or multiple images
- clip art or a different style of illustration
- contrived situations that are obviously staged, with awkward or uncomfortable-looking people dark, depressing, blurred or bland imagery obvious metaphors or clichés.

Departmental staff can access images on the Digital Asset Management System.

Department
for Education

Any enquiries regarding this publication should be sent to us at Publishing.TEAM@education.gsi.gov.uk

Department
for Education

Writing style guide

November 2016

Contents

About this guide

This is a step-by-step guide to writing communications for the Department for Education and its executive agencies.

It's important that we have single unified approach to writing and language. It helps people understand who we are, what we do and how we want to engage with them. It is as important as following a consistent design style.

Before you start producing written communications – whether that's web content, a publication or an email – please read this guide and adopt the principles outlined.

This guide should be used alongside the Government Digital Service (GDS) A to Z style guide. House style is a set of writing guidelines that organisations develop and use to ensure consistency in written communications. The A to Z clarifies questions such as when to capitalise words, and how to present bullet point lists. It replaces the department's intranet guide. The A to Z is regularly updated to include new education terms and to reflect linguistic changes that naturally occur over time.

This writing guide does not replace ministers' preferences for their own correspondence, submissions and briefings. Details of ministers' preferences are on the intranet.

Checklist – the six elements of good writing

1. Know your audience

Think about your subject from your reader's point of view. Consider your reader's workload, motivation and understanding.

2. Focus on the purpose

Be clear about what you want to achieve from your writing. Aim to sum up your reason for writing in a single sentence.

3. Plan a logical structure

List the points you want to make, then organise them into a clear structure. Do this with your audience and purpose in mind.

4. Write clearly, using plain English

Use everyday words and avoid using jargon. Keep sentences short and active. Be specific. Break up text with sub-headings.

5. Find the right tone of voice

This is open, positive, human and well-mannered.

6. Edit and proofread

Edit until you're satisfied. Get someone who is unfamiliar with the subject to do the final edit and proofread.

1. Know your audience

Before you start writing, think about what your reader needs and the questions they'll have. Whether you're writing for colleagues, ministers or an external audience, think about the subject from their point of view. A useful tip is to think of someone you know and write as if you're talking to them. It will sound much more natural.

Put yourself in the shoes of your reader and consider practical questions like workload, motivation and understanding. Ask yourself:

- How much time does my reader have for this?
- How can I make them want to read it?
- Will they understand technical terms and abbreviations?

2. Focus on your purpose

Be clear about this. Are you writing to inform, educate or persuade? What do you want to say? You must clearly understand what you want to say before you start writing.

Can you sum up your reason for writing in a single sentence? Use this sentence to help explain to readers what you're writing about at the beginning – this should be one of the first things you say.

3. Plan a logical structure

Spend time planning before you start and you'll save time later on. It will give you the confidence to decide what you can leave out. Organising your information in a logical order helps your writing to flow, and keeps you focused on the purpose. If you have a lot of material, a clear and coherent structure will help your reader engage more easily.

4. Write clearly, using plain English

- **Use plain English.** Don't use formal or long words when easy or short ones will do. Use everyday words that are used in conversation. Use 'buy' instead of 'purchase', 'help' instead of 'assist', 'about' instead of 'approximately' and 'like' instead of 'such as'. Remember you are trying to engage, rather than impress, readers.

- **Avoid using jargon**. We lose trust from our audiences if we use government 'buzzwords' and jargon that they find difficult to understand. If you need to introduce a technical term, make sure you explain it first, in plain English. The first time you use an abbreviation or acronym, explain it in full.

- **Be concise.** Leave out any unnecessary information. Keep sentences and paragraphs short. An average of 15 to 20 words per sentence is ideal.

- **Make your sentences active rather than passive**. Active sentences give your writing energy and clarity. They're quicker and easier to read and are more memorable. In active sentences the subject (the person or thing that is doing something) comes in front of the verb. You say *who* is doing *what*: "the Minister gave a speech" (active) not "a speech was given by the Minister" (passive).

- **Be open and specific**. Don't use words that are too general and vague (see the list of words to avoid on page 8), as this can lead to misinterpretation or empty, meaningless text.

- **Use direct language when you're giving instructions**. Commands will get your message across faster e.g. "follow these steps" and "read this information carefully". If you need to soften the tone of your instruction, say "please".

- **Use verbs**. Try not to turn verbs ("doing" words) into nouns. For example, say: "We will discuss this later", not "We will have a discussion about this later". Using too many nouns will make sentences longer and more complicated than they need to be.

- **Use sub-headings**. These are a good way of breaking up text into easy-to-manage chunks and they help you organise the points you want to make in a logical way.

5. Find the right tone of voice

When we speak, our tone of voice communicates a mood that adds meaning to the words we say. The tone we use will depend on our audience, purpose and subject matter. The department's tone is always open, positive, human and well-mannered.

Use positive words. Even if your message is a tough one, you can express it in a balanced and open way that takes account of your reader as a person.

Positive language tells the reader what is possible, is helpful (e.g. "can", "will", "do"), sympathetic and polite, and apologises where necessary.

Negative language implies the reader is at fault, doesn't suggest alternatives, expresses no sympathy, and may sound aggressive (e.g. "not possible", "does not have").

6. Edit and proofread

Allow plenty of time for proper editing and proofreading after you've completed your first draft.

Editing and proofreading tips:

- When editing, read your work out loud. Does it sound natural? Can you read whole sentences without running out of breath? This is a good way of checking whether sentences are too long, repetitive or full of jargon.

- Cut out any words you don't need. For maximum impact, use a minimum of words.
- Proofread from paper copies. On average you'll find 15 per cent more mistakes than when reading from a screen.
- Use a ruler under each line as you proofread. This will force you to slow down and read one word at a time. Reading from right to left also forces you to focus on the accuracy of the words rather than the meaning, which will help you spot more mistakes.
- Find quiet time and space to proofread properly. Don't treat it as an add-on.
- Tell yourself you want to find mistakes. You'll be more likely to find them.
- Ask someone who hasn't been involved in drafting to check for mistakes.

Words to avoid

We lose trust from our audiences if we write government 'buzzwords' and jargon. Often, these words are too general and vague and can lead to misinterpretation or empty, meaningless text. We can do without these words:

agenda (unless it's for a meeting)

advancing

collaborate (use 'working with')

combating

commit / pledge (we need to be more specific – we're either doing something or we're not)

countering

deliver (pizzas, post and services are delivered – not abstract concepts like 'improvements' or 'priorities')

deploy (unless it's software)

dialogue (we speak to people)

disincentivise (and incentivise)

empower

facilitate (instead, say something specific about how you are helping)

focusing

foster (unless it's children)

(to) impact (as a verb)

initiate

key (unless it unlocks something, it's probably 'important')

(to) land (as a verb. Only use if you are talking about aircraft)

leverage (unless in the financial sense)

liaise

overarching

(to) progress (as a verb – what are you actually doing?)

promote (unless you are talking about an ad campaign or some other marketing promotion)

robust

slimming down (processes don't diet – we are probably removing x amount of paperwork, etc)

streamline

strengthening (unless it's strengthening bridges or other structures)

tackling (unless it's rugby, football or some other sport)

transforming (what are you actually doing to change it?)

utilise

Always avoid metaphors. For example:

drive (you can only drive vehicles; not schemes or people)

drive out (unless it's cattle)

going forward (unlikely we are giving travel directions)

in order to (superfluous – don't use it)

one-stop shop (we are government, not a retail outlet)

ring fencing

With all of these words you can generally get rid of them by breaking the term into what you are actually doing. Be open and specific.

Writing for different communication channels

Writing for the web

We don't read from the screen in the same way as we read printed documents. Your web writing should reflect this. When reading on screen we:

read more slowly – about 25 per cent more slowly

scan the page instead of reading the whole document

want specific information – and fast

dip in and out of pages and sections of pages, a bit like reading a newspaper

don't read left to right or top to bottom.

Think about what your web user needs.

Summarise content in plenty of clear headlines and subheadings – it helps users find what they're looking for.

Put your most important point first and least important last – web users probably won't read to the end.

Keep sentences and paragraphs really short, with no more than one point in each paragraph.

Use links sparingly or separate them from the text.

GOV.UK

If you are writing content for GOV.UK, please follow the GDS A to Z style guide.

The intranet has more information about publishing content on GOV.UK.

Social media channels

Social media is informal, personal and direct. We use a simpler, more informal language style on our social media channels (Twitter, Facebook etc.) than in other departmental communications.

Writing letters

Have a clear structure. Begin by introducing your subject and responding to any previous letter. Then set out the points you want to make, answering any queries from your reader. Make sure you plan your writing so that it flows smoothly and logically from one idea to the next. You might want to set out your points in order of importance.

End your letter by telling the reader what they need to do next. Don't just sum up what you've already written. For example, you might say: "I hope this answers your question. If you need more information please contact..."

For more advice on drafting correspondence for each of our ministers, please read the details of their preferences on the intranet.

Writing emails

Take the same care with emails as you would for any other public communication. Emails aren't necessarily secure, and they are covered by the FOI Act.

Be friendly. Always judge you audience, but generally emails are less formal so it's usually OK to sign off with "Regards" rather than "Yours faithfully".

Be short. Learn to summarise.

Know your purpose. State it briefly in the subject line.

Be professional. Follow normal rules for spelling and grammar.

Be polite. It's more difficult to judge someone's tone from an email. Don't forget your manners in your hurry to send.

SCHEDULE 15: KEY SUBCONTRACTORS

Key Sub-contractors to be used by the Supplier in providing the Services to the STA:

Name of supplier	Services provided
Communisis UK Limited Company number 01006371	Printing Communisis will provide the printing of key stage 1 and 2 test papers. They will use the template that the STA provides to print the papers to their specifications and with the appropriate quality checks
Granby Marketing Services Limited Company number 03877685	Collation Granby will collate all tests papers ready for them to be delivered to the education institutions. They will package the papers according to quality standards
Royal Mail Group Limited trading as Parcelforce Worldwide Company number 4138203	Courier service Parcelforce will be responsible for the delivery to and collection of the test papers from the education institutions and ensuring that they arrive at the scanning facility
Civica UK Limited Company number 1628868	Online marking solution Civica will be responsible for the implementation and maintenance of the MarkManager software that will allow the markers to grade the test papers online
Scottish Qualifications Authority A non-departmental public body established under the Education (Scotland) Act 1996	Marking services SQA will be responsible for managing markers during Live Marking and acting as an advisor on education strategy

Notified Subcontractors:

None

SCHEDULE 16 – PART 1: APPROVED LOCATIONS – OPERATIONAL DELIVERY

The table below comprises the Approved Locations that will be used by the Supplier to provide the Services.

Other Supplier locations may be used from time to time for governance meetings.

Approved Locations for Operational Delivery

Name of supplier	Location(s)
Capita (Central Government Services Division) (operational management and contact centre)	Fort Dunlop, BIRMINGHAM, B24 9QT 30 Berners Street, LONDON, W1T 3LR
Capita (Transformation) (transition team)	17 Rochester Row, LONDON, SW1P 1JB Fort Dunlop, BIRMINGHAM, B24 9QT
Capita (Central Government Services Division - Document and Information Services (scanning house))	Lingfield Point, DARLINGTON, DL1 1ZQ Faverdale Industrial Estate, DARLINGTON, DL3 0QN
Capita (Central Government Services Division – Document and Information Services (printing of attendance registers)	7–11 Lower Oakham Way, MANSFIELD, NG18 5BY
Capita (Capita Software Services Division) (replacement for NCA Tools portal)	Anchor and Hope Lane, LONDON, SE7 7SN Birmingham Road, B80 7BG
Communisis (print supplier)	Manston Lane, LEEDS, LS15 8AH
Granby (collation supplier)	Stanley Street, BLACKBURN, BB1 3BW
Pia (specialist print supplier)	Victoria Street, CWMBRAN, NP44 3YT
Parcelforce (national hubs)	Middlemarch Business Park, COVENTRY, CV3 4HX Buckshaw Avenue, CHORLEY, PR7 7DW
Scottish Qualifications Authority	The Optima Building, 58 Robertson Street, GLASGOW, G2 8DQ
Civica (On Screen Marking Solution)	Brooke Park Estate, WILMSLOW, SK9 3PW Ball Green, Cobra Court, M32 2QT

SCHEDULE 16 – PART 2: APPROVED LOCATIONS FOR SET-UP

The table below comprises the approved locations that will be used by the Supplier to provide the Services. Other Supplier locations may be used from time to time for governance meetings.

Name of supplier	Location(s)
Capita (Central Government Services Division) (operational management and contact centre)	Fort Dunlop, BIRMINGHAM, B24 9QT 71 Victoria Street, LONDON, SW1H 0XA
Capita (Transformation) (transition team)	17 Rochester Row, LONDON, SW1P 1JB Fort Dunlop, BIRMINGHAM, B24 9QT
Capita (Central Government Services Division - Document and Information Services (scanning house))	Lingfield Point, DARLINGTON, DL1 1ZQ Faverdale Industrial Estate, DARLINGTON, DL3 0QN
Capita (Central Government Services Division – Document and Information Services (printing of attendance registers)	7–11 Lower Oakham Way, MANSFIELD, NG18 5BY
Capita (Capita Software Services Division) (replacement for NCA Tools portal)	Anchor and Hope Lane, LONDON, SE7 7SN Birmingham Road, B80 7BG
Communisis (print supplier)	Manston Lane, LEEDS, LS15 8AH
Granby (collation supplier)	Stanley Street, BLACKBURN, BB1 3BW
Pia (specialist print supplier)	Victoria Street, CWMBRAN, NP44 3YT
Parcelforce (national hubs)	Middlemarch Business Park, COVENTRY, CV3 4HX Buckshaw Avenue, CHORLEY, PR7 7DW
Scottish Qualifications Authority	The Optima Building, 58 Robertson Street, GLASGOW, G2 8DQ
Civica (Onscreen Marking Solution)	Brooke Park Estate, WILMSLOW, SK9 3PW Ball Green, Cobra Court, M32 2QT

This Agreement is made on [•] **between:**

(1) **The Secretary of State for Education** acting through the **Standards and Testing Agency of 53-55 Butts Road, Earlsdon Park, Coventry CV1 3BH** ("STA"); and

(2) **[Company's legal name]**, a company incorporated in [country/registration number] having its registered office address at [address] ("**Company**")

(each a "**Party**" and together referred to as the "**Parties**")

Background:

(A) STA has agreed to disclose the Confidential Information subject to the terms and conditions of this Agreement for the purpose of the Company [providing services/tendering to provide services] exclusively on behalf of STA (the "**Purpose**").

(B) In consideration of such disclosure, the Company has agreed to keep the Confidential Information confidential.

Now it is hereby agreed as follows:

1. **Definitions**

1.1 The following expressions shall have the following meanings unless the context otherwise admits:

"**Authorised Person**" means any director, officer, employee, subcontractor or professional advisor of the Company to whom disclosure of Confidential Information is reasonably necessary to fulfil the Purpose;

"**Business Day**" means a day other than a Saturday, Sunday or public or bank holiday in England;

"**Commencement Date**" means the date of signature of this Agreement;

"**Company Group**" means the Company and each company or entity in which the Company has a shareholding or interest, directly or indirectly, of 50 per cent or more or has the right to exercise, directly or indirectly, 50 per cent or more of the voting rights;

"**Confidential Information**" means any commercial, financial, business and technical, marketing or other data, including business methods, know-how, trade secrets, diagrams, specifications, calculations, formulae, algorithms, processes, models, drawings and all other confidential information of whatever nature (in any form or medium) of STA or its third party suppliers given or made available by STA to the Company in connection with the Purpose;

"**Environmental Information Regulations**" means the Environmental Regulations 2004 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the UK Information Commissioner in relation to such legislation;

"**FOIA**" means the Freedom of Information Act 2000 (as amended) and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the UK Information Commissioner in relation to such legislation;

"**Information**" has the meaning given under section 84 of the Freedom of Information Act 2000;

"**LCIA**" means the London Court of International Arbitration;

"**Purpose**" has the meaning given in the Recital; and

"**Request for Information**" a request for information or an apparent request under FOIA or the Environmental Information Regulations.

2 Structure and Process

This Agreement sets out the terms on which STA shall make the Confidential Information available to the Company and on which the Company shall use such Confidential Information.

3 Term

This Agreement shall take effect from the Commencement Date and shall continue for a period of seven years thereafter.

4 Confidentiality Obligations

4.1 In consideration of the disclosure of Confidential Information as contemplated in this Agreement, the Company shall:

4.1.1 keep the Confidential Information confidential subject to the terms and conditions of this Agreement;

4.1.2 not disclose the Confidential Information or any part thereof to any person other than an Authorised Person, and shall ensure that each such Authorised Person shall comply with confidentiality provisions no less onerous than those contained in this Agreement;

4.1.3 not use the Confidential Information or any part of it for anything other than the Purpose;

4.1.4 not copy, summarise or transcribe the whole or any part of the Confidential Information, save as is reasonably necessary for the Purpose and all such copies, summaries and transcripts shall be deemed to be, and shall be clearly identified as being, Confidential Information;

4.1.5 keep all Confidential Information in a safe and secure place and shall treat all Confidential Information in a manner which is no less secure than the manner in which it treats its own confidential and/or proprietary information and at least with reasonable care;

4.1.6 notify STA immediately on it becoming aware that any Confidential Information has been disclosed to or is in the possession of any person who is not an Authorised Person;

4.1.7 upon termination of this Agreement or at the request of STA, deliver up to STA or destroy or erase (as STA may in its absolute discretion direct) any records of whatsoever nature which are in the possession, custody or control of the Company to the extent that such records contain any Confidential Information or which are produced or received by the Company in connection with the Purpose, except to the extent that the same form part of the permanent records of the Company which it is bound by law or regulatory requirement to preserve, and the provisions of this Agreement shall, notwithstanding its termination, continue to apply to all such retained Confidential Information; and

4.1.8 upon request provide to STA written confirmation that the provisions of Clause 4.1.7 have been fully complied with.

4.2 All Confidential Information shall be deemed to be (and all copies thereof or of any part or parts thereof shall become upon the creation thereof) and shall remain the property of STA and its third party suppliers.

5 Exclusions

5.1 Notwithstanding any other provisions hereof, the Company shall not be liable for the release or disclosure of, and the confidentiality obligations hereunder shall not apply to, any Confidential Information that is:

5.1.1 part of or enters the public domain through no fault of the Company and without breach of this Agreement;

5.1.2 subsequently obtained by the Company from a third party without breach of any obligation of confidentiality owed to any third party or STA;

5.1.3 known to the Company prior to the disclosure by STA without an obligation to keep such Confidential Information confidential;

5.1.4 approved in writing for public release by STA; or

5.1.5 independently developed by the Company or a person within the Company Group as evidenced by written records and without any breach of this Agreement.

5.2 The Company may disclose Confidential Information in accordance with a judicial or other governmental order or a regulation of a regulatory authority to whose jurisdiction the Company submits, provided that the Company:

5.2.1 uses its reasonable endeavours to obtain prior to the disclosures a written assurance from the applicable judicial or governmental authority that it will afford the Confidential Information a reasonable degree of protection against disclosure; or

5.2.2 gives STA reasonable notice prior to such disclosure to allow STA a reasonable opportunity to seek a protective order or otherwise.

6 Freedom of Information

6.1 The Company acknowledges that STA is subject to the requirements of FOIA and the Environmental Information Regulations and shall assist and co-operate with STA to enable STA to comply with its Information disclosure obligations.

6.2 The Company shall, and shall procure that members of the Company Group shall, at STA's reasonable cost:

6.2.1 transfer to STA all Requests for Information that it receives as soon as practicable and in any event within 3 Business Days of receiving a Request for Information;

6.2.2 provide STA with a copy of all Information in its possession or power in the form that STA requires as soon as practicable on a rolling daily basis and in any event completely within 10 Business Days (or such other period as STA may specify) of STA's request; and

6.2.3 provide all necessary assistance as reasonably requested by STA to enable STA to respond to any Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations,

provided always in respect of Clauses 6.2.2 and 6.2.3 that STA shall first use its reasonable endeavours to respond to the request using its own records prior to seeking assistance from the Company.

6.3 In no event shall the Company respond directly to a Request for Information unless expressly authorised to do so in writing by STA.

7 Intellectual Property Rights

This Agreement shall not operate as an assignment of any patents, copyrights, registered designs, unregistered designs, trademarks, trade names or other rights as may subsist in or be contained in or reproduced in the Confidential Information and the Company shall not, nor shall any persons on its behalf, apply for any patent, or registration of any trade mark or design or any other intellectual property right, in respect of the Confidential Information or any part thereof.

8 Publicity

Neither Party will make any announcement or disclosure concerning or touching upon the subject matter of this Agreement, without the prior written consent of the other Party.

9 Liability

9.1 The Parties acknowledge that:

9.1.1 Confidential Information may relate to highly sensitive aspects of the business of STA;

9.1.2 any loss, misuse or unauthorised disclosure of the Confidential Information or any part of it will or may be damaging to the interests of STA and will or may significantly damage its relationships with its third party suppliers;

9.1.3 financial compensation may not adequately compensate STA for any such damage,

and accordingly the Company acknowledges the right of STA to seek injunctive relief, whether interim or final, against the Company or any Authorised Person in the event of any threatened or actual breach of the terms of this Agreement by the Company or any of its Authorised Persons.

9.2 The rights of STA under the foregoing Clause 9.1 shall be in addition to STA's other rights in law or in equity.

9.3 The Company shall, as and when requested by STA, do all acts and execute all documents as may be reasonably necessary to prevent any loss, misuse or unauthorised disclosure of the Confidential Information or any part of it by any of its Authorised Persons.

9.4 The Company shall remain liable for any disclosure of Confidential Information by any Authorised Person as if it had made such disclosure itself.

10 Assignment

The Company shall not assign, novate or otherwise transfer this Agreement to any person without the prior written consent of STA.

11 Disclaimer

STA makes no representations or warranties as to the accuracy or completeness of the Confidential Information disclosed.

12 General

12.1 This Agreement constitutes the entire agreement between the Parties with respect to the subject-matter of this Agreement and (to the extent permissible by law) supersedes all prior representations or oral or written agreements between the Parties with respect to that subject matter, provided that neither Party is attempting to exclude any liability for fraudulent

statements (including fraudulent pre-contractual misrepresentations on which the other Party can be shown to have relied).

12.2 An amendment of this Agreement will not be binding on the Parties unless set out in writing, expressed to amend this Agreement and signed by authorised representatives of each of the Parties.

12.3 No failure of either Party to exercise, and no delay by it in exercising, any right, power or remedy in connection with this Agreement (each a "**Right**") shall operate as a waiver of that Right, nor shall any single or partial exercise of any Right preclude any other or further exercise of that Right or the exercise of any other Right. A waiver may be made only in writing and must be expressly stated to be a waiver of a Party's rights under this Agreement.

12.4 This Agreement shall be enforceable by respective successors, transferees and assigns of STA and the Parties agree that the Company's obligations and liabilities shall not be discharged, lessened or extinguished by way of any succession of, transfer by or assignment by STA of its rights under this Agreement and this Agreement shall continue in full force and effect on any such succession, transfer or assignment and the Company shall perform it obligations and owe its liabilities in favour of any such successor, transferee or assignee of STA as if such successor, transferee or assignee was appointed as a party to this Agreement ab initio and benefits from the same rights and entitlements as STA hereunder.

12.5 This Agreement does not create any right or benefit enforceable by any person not a party to it or contemplated by Clause 12.4 (within the meaning of the Contracts (Rights of Third Parties) Act 1999).

12.6 The invalidity or unenforceability of any part of this Agreement for any reason whatsoever shall not affect the validity or enforceability of the remainder.

12.7 This Agreement may be entered into in any number of counterparts all of which, when taken together, shall constitute one and the same instrument. Any Party may enter into this Agreement by executing any such counterpart.

13 Governing Law and Arbitration

13.1 This Agreement and any disputes arising under it shall be governed by and construed in accordance with the laws of England and Wales.

13.2 Any dispute arising out of or in connection with this Agreement, including a dispute as to the validity or existence of this Agreement and/or this Clause 13 shall be resolved by arbitration in London conducted in English and in accordance with the rules of the LCIA by a single arbitrator who shall be appointed by the LCIA.

13.3 The arbitrator shall be and remain independent and impartial of each Party.

13.4 An award rendered in connection with arbitration pursuant to this Clause 13 shall be final and binding upon the Parties, and any judgment upon such an award may be entered and enforced in any court of competent jurisdiction.

14 Functions and Powers

Nothing in this Agreement shall be construed as limiting or fettering STA's powers to liaise with or investigate or request, receive or disclose information from the Company in STA's capacity.

In witness whereof this Agreement has been duly executed:

SIGNED for and on behalf of **STA**

by:

SIGNED by .....

for and on behalf of **[COMPANY NAME]**

having been duly authorised to do so

This Schedule sets out the Data, Software and Materials used in the delivery of the Services, grouped using the definitions shown in Clause 1 (Definitions and Interpretations).

COTS Third Party Software

The table below is the COTS Third Party Software that the Supplier will use under this Agreement, showing the name of the software, the supplier of the software and the business function that is used for.

Software	Supplier	Business Function
SharePoint	Microsoft	Repository for project management documentation
Microsoft Office	Microsoft	Project and programme management, general office administration e.g. email
Folding Space	Folding Space	Warehouse management
Kofax	Lexmark	Scanning and indexing
Avaya	Avaya	Telephony platform for contact centre
Verint	Verint Systems	Call recording in the Contact Centre
Asigra	Asigra	Back-up data held on Advantage Digital platform
Alien Vault	Alien Vault	Security information event monitoring
Click 4 Assistance	Click 4 Assistance	Webchat in support of the TOpS Portal
PCA Predict	PCA Predict	Address verification

Specially Written Software

None.

Supplier Software

Software	Supplier	Business Function
One Digital	Capita	Master data repository including the Test Operations Services database as found in the TOpS portal

Third Party Software

The COTS Third Party Software listed above and the following:

Software	Supplier	Business Function
MarkManager	Civica	Onscreen Marking solution

STA Data

The table below contains a list of STA Data.

STA Data Item	Description
1	Marker Register*
2	Datafeeds*
3	Test Orders*
4	Test Results*
5	Teacher Assessment*
6	Other data contained in datafeeds made to STA pursuant to or in connection with the Agreement
7	Standards Maintenance* data
8	Data contained in Supplier, Subcontractor, Marker or STA interactions and/or communications with or to Schools (including Test Order transactions and reports received via helpdesks)
9	Data relating to Pupils
10	Content relating to websites
11	Management Information*
12	Head teacher Declaration* (HDFs)
13	Data relating to Schools
14	Database history relating to any Helpdesks
15	Where not otherwise included in the above list all further School, Pupil and Test Results data held by the Supplier within any software application.
16	Any data produced by the Supplier or any Subcontractor in the performance of the Services or provided by STA at any time shall be STA data unless otherwise agreed in Product Descriptions and Exit Plans, or by other mechanisms used from time to time.

*As defined in Appendix 2 of Part 1 (Statement of Requirements) of Schedule 4 (Services).

STA Materials

The table below contains a list of STA Materials.

STA Material Ref	Description
1	National Curriculum Assessments*
2	Product Descriptions
3	Set-up Project Initiation Document (PID)
4	Operational Delivery Project Initiation Document (PID)
5	Correspondence – with STA
6	Correspondence – with Regulatory Authorities
7	Correspondence – with Schools
8	Correspondence – with Markers
9	Training materials, including Marker Training Materials
10	Advertising literature
11	Marketing literature
12	Any Materials produced by the Supplier or any Subcontractor in the performance of the Services or provided by STA at any time shall be STA data unless otherwise agreed in Product Descriptions, Exit Plans, or by other mechanisms used from time to time.

* As defined in Appendix 2 of Part 1 (Statement of Requirements) of Schedule 4 (Services).

STA Software

The table below contains a list of STA Software.

STA Software	Description
N/A	N/A